وزارة التعليم العالي والبحث العلمي

جامعة محمد خيضر ــ بسكرة

كلية الحقوق والعلوم السياسية

قسم الحقوق

الموضوع:

الحماية الجنائية للتجارة الإلكترونية

أطروحة مقدمة لنيل شهادة دكتوراه علوم في الحقوق

تخصص: قانون جنائي

إعداد الطالب:

بن شهرة شول

تحت إشراف:

الأستاذ الدكتور علي أجقو

أمام لجنة المناقشة المكونة من السادة الأساتذة:

عمر فرحاتي	دكتوراه	أستاذ	جامعة بسكرة	رئيســـــا
علي أجقو	دكتوراه	أستاذ	جامعة بسكرة	مقررا
عبد الحفيظ طاشور	دكتوراه	أستاذ	جامعة قسنطينة	ممتحنا
رشيدة العام	دكتوراه	أستاذ محاضر "أ"	جامعة بسكرة	ممتحنا
حورية لشهب	دكتوراه	أستاذ محاضر "أ"	جامعة بسكرة	ممتحنا
شادية رحاب	دكتوراه	أستاذ محاضر "أ"	جامعة باتنة	ممتحنا

السنة الجامعية: 2011/2010

المقدمـــــــــة:

يتسق تماما صيرورة البشرية في خطها الزمني تسارع مسارها في المجال التكنولوجي، فبعلمنا أنه عقد بعد عقد يستحدث من الوسائل و الآليات ما يعتبر بهما ما مضى تقليديا في كل جوانب النشاط البشري، و لما كان الاتجار أحد هذه الجوانب فهو لا محالة متأثر بكل تطور حادث و مستفيد منه فمن غير الممكن أن يبقى النشاط التجاري محصورا بوسائله التقليدية دون استخدام آليات هذه التكنولوجيا لئلا يحكم على فاعليته بالجمود و يستحيل تصور ذلك.

و من أبرز ما توفره المعلوماتية في المجال الالكتروني أو ما يعرف مؤخرا بالتجارة الالكترونية من مزايا يتقاسمها طرفا التعامل و التعاقد أنها بالنسبة للمتعاملين أو الزبائن توفر الجهد و حرية الاختيار و خفض التكلفة و نيل رضا المستخدم أما بالنسبة للشركات و المؤسسات فإنها تعتبر بحق عامل تسويق أكثر فعالية كما تعمل على تخفيض مصاريف الشركات و خلق تواصل فعال مع الشركاء و العملاء، كون التجارة الالكترونية تعتمد تأخذ صورة التجارة عبر الانترنيت أو ما يسمى التعاقد عن بعد تتمركز في عملياتها شبكة الانترنيت و تأخذ دورا محوريا تنساب بواسطتها مليارات من العملات و بلايين.

من صالح الكل أن يباع و الآخر أن يتسوق دون أن يتكلف مشقة التنقل و عرض السلع و معاينتها موضعيا. فميزة هذه الطفرة التكنولوجية أن كل عمليات الاتجار من عرض و طلب و معاينة و حتى تغيير المواصفات تتم الكترونيا و بنفس الطريقة يكون السداد مقابل الوفاء

و لما كانت طبيعة هذا النشاط ترتكز على ركني السرعة و الائتمان فإن الركن الأول توفر إلى حد جعل التساهل أو التباطؤ عن جدية التعامل معهم لا تؤمن فيه العواقب لما له من تأثير على المجال الحيوي و الحياتي و الأمني لا للأفراد فقط بل حتى على مستوى الأمن القومي للكيانات الدولية و أصبح يؤثر حتما على الركن الثاني للأعمال التجارية – الائتمان – و بقدر حاجة التجارة و الأعمال التجارية إلى السرعة و خدمة الأخيرة للأولى فإن الائتمان يظل مفتاح العملية فإن أبرز ما يتهدده ما يعرف بالجريمة الالكترونية حيث تصبح و تبقى عقبة حقيقية في وجه تمام هذه التجارة فالحد

الثاني في المعادلة التجارية و هو المستهلك أو المتعامل بحاجة إلى كسب ثقة و اطمئنانه للتسوق و الاتجار بعيدا عن المتجر التقليدي فمن المشاكل ما يتعلق بوسائل و صور حمايته وسواء ما تعلق ببياناته الخاصة و تعاملاته البنكية و بطاقات الائتمان و حمايته من استغلال تلك البيانات قصد النصب أو خيانة الأمانة و كل استعمال غير مشروع، و كذا المؤسسات بخطر الدخول لمواقعها و التغيير في بياناتها و حساباتها، فضلا عن جريمة التهرب الضريبي و الجبائي.

فالمشرع القانوني و إن اجتهد فعلا في تطويق و تأطير هذا المجال الحيوي بكل حماية القانونية و قررها إلا أن هذا التسارع في مجال التكنولوجيا من استحداث وسائل المواصلات أولا ثم آليات الاتصالات – شبكة الإنترنيت – يظهر أنه يسبق قدره المشرع و يتجاوز اجتهاداته في تقرير أي حماية للحقوق لما يتسم به هذا التسارع و ما تتميز به هذه الثورة من خصائص تجعلها بحق ظاهرة يعجز الواقفون وراء بعثها عن السيطرة عنها و بالتالي مهددا لكثير من المراكز القانونية.

الصعوبـــــــــات:

صعوبة بعض عناصر البحث لاتصاله بجوانب فنية تتسم بالدقة و الصعوبة حيث تستوجب الإحاطة ببعض المعارف و المعلومات التخصصية و بعض الجوانب التقنية و الفنية لشبكات الاتصال و نظم المعلوماتية و آليات المعالجة الآلية لنظم المعلومات، و استخدامات الحواسيب (برامج، فيروسات) حيث من الصعوبة بمكان لمن يتصدى لدراسة مثل هذه المواضيع البحث فيها دون الإلمام أو الحصول على حد أدنى من المعرفة التقنية بنظم المعلوماتية و الحواسيب لإدراك أكبر توفيق في إيجاد حلول للمشاكل القانونية التي تطرحها معاملات هذا النشاط (التجارة الالكترونية).

حداثة مثل هذه المواضيع حيث صدر أول مشروع دولي ينظم هذه معاملات عام 1996 و هو القانون النموذجي.

و لا يزال المشرع في أي دولة يحاول جاهدا الإحاطة بأثر الإجرام المعلوماتي و تحديث نظمه القانونية و الجنائية لتتوافق مع ذلك الأثر الذي أحدثته و مازالت تحدثه تكنولوجيا المعلومات.

امتداد أثر العلم الافتراضي إلى العالم المادي.

تعلق الدراسة كحماية مصالح جديدة (مستحدثة)، هذه المصالح هي من ذات طبيعة الآلية أي أنها ذات طابع غير.

الأهميـــــــــة:

لكل تطور تقني و تكنولوجي انعكاساته على الكيانات و المراكز القانونية بصفة عامة، و على القانون الجنائي بوجه خاص، حيث لمستخرجات الحديثة (الالكترونية) و مع ازدياد قوة الارتباط و الاحتياج لها يتطلب تلك المراكز القانونية حماية جنائية سواء بإقرارها بالنصوص التقليدية أو باستحداث النصوص الملائمة لطبيعتها و خصوصيتها و تبتدي أهمية هذه الحماية من صلة

- حماية الحقوق المنصوص عنها دستوريا في كافة التشريعات و ضمانات هذه الحقوق في مواجهة الاعتداء عليها أثناء أو في إطار العلاقة التعاقدية الالكترونية التجارية و يأتي على رأس أهم هذه الحقوق الحق في الخصوصية أو حماية الحياة الخاصة.

- ضرورة إقرار أو تحقيق التوازن الضروري بين مصلحة المجتمع في اعتماد هذه الآلة الحديثة كتقنية لتسهيل المعاملات التجارية و اختزال المسافات و اختصار الوقت و بين مصلحة المتعاملين بها سواء أكان أطراف العلاقة التعاقدية التجارية كأن يكونوا مستهلكين لهم الحق في حماية حياتهم الخاصة و أسرارهم و ضعف مراكزهم في تلك الرابطة، أو كانوا حرفيين فلهم الحق في حماية نظم معاملاتهم، و أموالهم، كما يتوجب حماية حق الدولة في جباية مستحقاتها الضريبية. بكل هذه العناصر تشكل مصلحة اجتماعية تستحق التدخل لتحقيقها حماية جنائية بإقرار نصوص تجريمية و عقابية لها بشقيها الموضوعي و الإجرائي.

- ضرورة إقرار نظم وقائية في أحسن الأحوال لمحاولة مسايرة التطور التكنولوجي و ليس لاستباقه – فهذا طرح ربما غير منطقي – من منطلق أن الجريمة قرينة التكنولوجيا بالقدر الذي يستفيد فيه النشاط الإنساني عموما و

النشاط التجاري على وجه الخصوص من تقنية شبكة الانترنيت و الحواسيب بقدر أكبر يوصف الإجرام المعلوماتي كفاءاته و اقتداره لتعظيم مكاسبه و تحقيق أهدافه الجرمية، و هذه

- الجرائم الالكترونية أو المعلوماتية هي الآن ظاهرة العصر و هي أقوى تحدي يواجه القانون الجنائي على وجه الخصوص إذا ما نظر على وجه المقارنة بين عظم المكاسب التي تتحقق بفعل انخراط النشاط التجاري في المنظومة الرقمية و بين حجم الخسائر التي يتعرض لها قطاع الأعمال (مؤسسات مالية، بنوك، مصارف، شركات تجارية، وسطاء...) على أن هذه الخسائر قد تكون أفدح في حق الطرف الأضعف في عقود التجارة الالكترونية.

- الاهتمام المتنامي لدى التشريعات المقارنة بموضوع هذا النشاط و محاولة هيكلته و تنظيمه وفق أطر قانونية ثم إحاطته بحماية جنائية موضوعية و إجرائية و لا يتعلق الأمر فقط بالدول الصناعية الكبرى أو المتقدمة بل إن في المشرع العربي نماذج ناجحة في هذا المجال و إن كانت في بدايتها فعلى سبيل المثال المشرع.

- مكنت سهولة الوصول إلى المعلومات في النظم المعلوماتية إلى اصطناع فضاء معلوماتي يفترض فيه كأصل عام الاستخدام الشرعي، لكن سوء استخدامه غير وارد فقط بل واقع يوجب التصدي له، مكان من الأهمية بمكان أن تظهر من الأهمية بمكان أن تظهر من خلال هذه الدراسة دعوة للنظم الجنائية إلى المحافظة على مسايرتها، و تحديث قواعدها التجريمية و العقابية حتى تستوعب مثل هذه السلوكيات.

- صعوبة تطبيق النصوص التقليدية على جرائم التجارة الالكترونية مما دفع بكثير من الدول إلى التدخل التشريعي لصد هذه الاعتداءات.

نطـــاق الدراســـة:

هذه الدراسة تعنى بالتعريف على الجرائم الواقعة على المعاملات التجارية الالكترونية باعتبارها محل نشاط إنساني حديث لارتباطه بتكنولوجيا حديثة و هي تكنولوجيا المعلوماتية أو الرقمية.

فاتصال أو الدمج الواقع أو التفاعل الواقع بين المعلوماتية كآلية عمل و بين النشاط التجاري كشف عن محصلة حديثة و هي معاملات التجارة الالكترونية التي كان لها دور في ظهور نمط جديد من السلوكيات الجرمية (الإجرامية)، مما استتبع ظهور محاولات إيجاد حلول قانونية لحماية تلك المراكز التي تنشأ عن التعاقد بواسطة هذه الآلية و هذا ما يؤكد الحاجة إلى تجريم كل الأفعال التي تشكل اعتداء على الحقوق...

و نتناول في البحث موضوع الجرائم الواقعة على المعاملات التجارية الالكترونية، من خلال دراسة مقارنة للأنظمة القانونية المختلفة، و نوضح فيها الأحكام العامة للجرائم لواقعة على معاملات التجارة الالكترونية، و ما مدى صلاحية النصوص التقليدية للتطبيق على هذه الجرائم و نحاول شرح العناصر التي تتألف فيها هذه السلوكيات الإجرامية.

نشير إلى أن دراسة الجرائم الواقعة على التجارة الالكترونية يطال كذلك التعرض للأحكام المتعلقة بالجرائم الالكترونية في كثير من مواضع هذه الدراسة (الاعتداء على نظم المعلومات، الاعتداء على الحياة الخاصة البيانات..... و الاسمية، الخدمات الوسيطية) بالإضافة..... جرائم التجارة الالكترونية بمواضيع تكون نسبيا حكرا عليها (ج التوقيع الالكتروني، ج المستهلك الالكتروني، ج التهرب الضريبي،...)

ثم إن نطاق هذه الدراسة يشمل البحث في القواعد الموضوعية الخاصة بجرائم التجارة الالكترونية كما يمتد ليشمل الأحكام الإجرائية أيضا للإسهام في فتح تصور أشمل و أوضح للسياسة الجنائية المتصدية لما استحدث على صعيد ظاهرة الإجرام.

الباب الأول:

الحماية الجنائية الموضوعية للتجارة الالكترونية

تمهيد:

تبعا لاحترام مبدأ الشرعية الجنائية فانه من الضروري عند بحث نطاق الحماية الجنائية لأي من المراكز القانونية، وجب البحث في مدى توفر أو تطابق أركان الجريمة على أي سلوك يشكل تهديدا لهذه المراكز، أو اعتداء عليها فعلا و هذا ما تتضمنه مدارسة الأحكام الموضوعية للحماية الجنائية، بالرغم من وجود تحدي كبير نتيجة هذه الثورة المعلوماتية و هو مثال تتجلى فيه صورة التعقيد في تأطير هذه المعاملات التجارية متمثل في كون أن مستعمل شبكة الانترنيت يستطيع في ذات الوقت أن يكون منتجا و وسيطا و مستهلكا و هذا التعدد في الأدوار يخلق أحيانا صعوبة جمّة في إسناد المسؤولية وتحديد قواعد القانون واجب التطبيق.[1]

و فضلنا أن تتضمن دراسة هذه الأحكام التعرض لبعض الأفعال التي تشكل تهديدا أو اعتداءا على مراكز قانونية في المعاملات في التجارة الالكترونية و ذلك وفق تقسيم هذا الباب ليشمل ثلاثة فصول، خصص الأول فيه للتعرض لبيان الإطار المفاهيمي لمعاملات التجارة الالكترونية كونها محل الدراسة أولا، ثم لحداثة هذه المعاملات على صعيد الممارسة و النشاط و التداول.

ثم خصص الفصل الثاني لدراسة نطاق الحماية الجنائية التي ينبغي أن يشمل أو تطال نظام عمل التجارة الالكترونية من ناحية موضوعية و دراسة أركان الجرائم الواقعة عليها و مدى كفاية القواعد التقليدية لتوفير حماية لها.

أما الفصل الثالث فتطرقنا فيه لنطاق الحماية الجنائية لمضمون النشاط التجاري الالكتروني بالتعرض لأهم ركائز هذا النشاط التي ظهر عليها تكييف حديث عن التقليدي منه. و نبين فيه الإشكالات الواردة في هذا المجال و الحلول المقترحة لها من وجهة نظر الفقه الجنائي و التشريعات المقارنة.

---

[1] -Isabelle Falque – Pierrotion, **Internet Enjeux juridiques, Rapports officiel**, Paris 1997, p53.

الفصل الأول

الإطار التنظيمي للتجارة الإلكترونية

من مميزات هذا العصر هو الثورة التكنولوجية وبالأخص ظهور طفرة الإنترنت في علم الاتصال مما يجعل البعض يسمي هذا العصر أو يضفه بأنه العصر الرقمي أو الافتراضي، الذي كان فيه انتشار الإنترنت بصورة هائلة، لم يعد مقتصرا على مجال البحث العلمي بل قد تم استخدامه تقريبا في جميع المجالات من أهم استخداماته في النشاط التجاري الذي أدى إلى ظهور احتياجات جديدة. فبفضل الإنترنت ظهرت أنشطة تجارية أخرى، ومنه شاع مفهوم التجارة الإلكترونية وأصبح أكثر الموضوعات أثارة للجدل القانوني في عصر المعلومات، وفي وقتا الحاضر أصبح أخر إفرازات عصر المعلومات وأكثرها اهتماما، غم ما سبقتها من موضوعات من أهمها: الخصوصية وحماية الحياة الخاصة من المخاطر التقنية التي كانت أول الموضوعات في أواخر الستينات وتتبعها جرائم الكمبيوتر ويليه الملكية الفكرية وغيرها، أما ولادة التجارة الإلكترونية جاءت لاحقا وأخر هذه الموضوعات، وذلك في منتصف التسعينات في أواخر التسعينات بشكل دقيق. فتعتبر التجارة آخر درجات التطور التاريخي لموضوعات تقنية المعلومات فهي تثير تحديات في سائر المجالات والموضوعات المشار إليها أمن المعلومات التعاقد إلكتروني، وسائل الدفع الإلكتروني ... إلخ ولقد وضعت عدة تعار يف للتجارة الإلكترونية فكان لدى بعض محصورا في بيع المنتوجات من المنتج إلى المستهلك عن طريق المراسلة باستخدام الإنترنت.

إلا أن نظرة هؤلاء جد ضيقة، فما المقصود بالتجارة الإلكتروني ة؟ إن إعطاء تعريف محدد وشامل لتجارة الإلكتروني ة ليس أمرا سهلا لأنه يتطلب إهتماما كبيرا بالعناصر التي تتضمنها والخصائص التي تتمتع بها وآلية عملها وتنظيمها القانوني.

ولهذا قسمنا هذا الفصل إلى ثلاثة مباحث، تطرقنا في المبحث الأول إلى مفهوم التجارة الإلكترونية، أما المبحث الثاني تناولنا فيه أحكام عقد التجارة الإلكترونية، أما المبحث الثالث، فكان في الإشكالات التي تقع في التجارة الإلكترونية.

المبحث الأول: مفهوم التجارة الإلكترونية

تناولنا في هذا المبحث إلى مفهوم التجارة الإلكترونية، فقسمنا هذا المبحث إلى ثلاثة مطالب: المطلب الأول هو تعريف التجارة الإلكترونية في بعض التشريعات العربية والأوروبية. المطلب الثاني هو أشكال التجارة الإلكترونية. والمطلب الثالث هو خصائص التجارة الإلكترونية.

المطلب الأول: تعريف التجارة الإلكترونية

قبل التطرق الى تعريف التجارة الإلكتروني ة يجب أن تبين أن مفهوم التجارة الإلكترونية يتكون من مقطعين:

الأول: التجارة "Commerce" وهذا المقطع يعبر عن نشاط تجاري واقتصادي معروف لدينا ويتم من خلاله تداول السلع والخدمات وفقا لقواعد ونظم متبعة ومتفق عليها.

الثاني: الإلكترونية "Electronique." والمقصود به هو القيام بأداء النشاط الاقتصادي "التجاري" باستخدام تكنولوجيا الاتصالات الحديثة مثل شبكة الإنترنت والشبكات والأساليب الإلكترونية.1

ولقد وضعت عدة تعاريف للتجارة الإلكترونية، ومع ذلك، أيا كان التعريف، فالمهم هو التركيز على خصوصية الوسيلة المستخدمة في التعاقد، وهي شبكات الاتصال التي يتم من خلالها هذا النوع من التجارة وبشكل خاص (الانترنت)

القانون النموذجي الذي وضعته الإنسترال(UNICITRAL):

لم يعرف التجار ة الإلكترونية وإنما عرف رسالة البيانا ت (Data Message) في المادة (ا.2) على أنها "المعلومات التي يتم إنشاؤها أو إرسالها أو استلامها وتخزينها

---

[1]–د. محمد سعيد أحمد إسماعيل، أساليب الحماية القانونية لمعاملات التجارة الإلكترونية، رسالة دكتورة، ". ط 2005. ص11.

بوسائل إلكترونية أو ضوئية أو بوسائل مشابهة مثل تبادل البيانات الإلكترونية أو البريد الإلكتروني أو التلكس أو النسخ البرقي" [2]

عرفتها المجلة العالمية للتجارة الإلكترونية: "هي بباسطة مصطلح يقصد به عمليات بيع وشراء وتسليم السلع وطلبها من منتجها أو بائعها ليس بالطريق ة العاديةِ وإنما إلكترونيا، وعادة ما تتم هذه العمليات عن طريق شبكة الانترنت".3

القانون التونسي للمبادلات والتجارة الإلكترونية لسنة 2000 :

عرف التجارة الإلكترونيةِ في الفصل الثاني من الباب الأول على أنها: "العمليات التجارية التي تتم عبر المبادلات الإلكترونية" وعرف المبادلات الإلكترونية في نفس الفصل على أنها المبادلات التي تتم باستعمال وثائق إلكترونية.

قانون المعاملات الإلكتروني الأردني لسنة2001:

لم يعرف التجارة الإلكترونية وإنما عرف المعاملات الإلكترونية في المادة (02) على أنها المعاملات التي تنفذ بوسائل إلكترونية كتقنية استخدام الوسائل كهربائية أو مغناطيسيةِ أو ضوئية أو إلكترومغناطسية أو أية وسيلة مشابهة في تبادل المعلومات وتخزينها.

وفي فرنسا:

شكلت مجموعة عمل برئاسة وزير الاقتصاد الفرنسي حيث عرفت التجارة الإلكترونية على أنها "مجموعة المعاملات الرقمية المرتبطة بأنشطة تجارية بين المشروعات بعضها مع بعض، وبين المشروعات والأفراد، وبين المشروعات والإدارة. 4

---

[2]– نضال إسماعيل برهم، أحكام عقود التجارة الإلكترونية، دار الثقافة لنشر والتوزيع عمان ط . 2005 ص 15

[3]– د محمد سعيد أحمد إسماعيل، نفس المرجع، ص: 15.

[4] - نضال إسماعيل برهم. مرجع سابق الذكر ص:15– 16.

قانون المعاملات الإلكترونية في إمارة دبي : وقد عرفها في هذا القانون على أنها "المعاملات التجارية التي تتم بواسطة المراسلات الإلكترونية.5

وقد ورد في المادة الأولى من مشروع قانون التجارة الإلكترونية المصري تعريفا لها بأنها "كل معاملة تجارية تتم عن بعد باستخدام وسيلة إلكترونية".6

ومن كل هذه التعريفات نستخلص أن التجارة الإلكترونية هي كل العمليات التجارية من بيع وشراء وتسليم البضائع التي تتم إلكترونيا عبر شبكة الانترنت.

المطلب الثاني: أشكال التجارة الإلكترونية:

يمكن تقسيم نشاطات التجارة الإلكترونية بشكلها الحالي إلى أقسام أساسية هي:7

من أعمال إلى أعمال: Business to business: تختصر في (b 2 b)* وهذا النمط يتم بين مؤسسات الأعما ل بعضها البعض من خلال شبكات الإتصالات وتكنولوجيا المعلومات، وذلك لتقديم طلبات الشراء للموردين والعارضين، وتسليم الفواتير وإتمام عمليات الدفع وهذا النمط من التجارة الإلكترونية موجودة منذ سنوات عديدة، خاصة في تبادل البيانات الإلكترونية من خلال الشبكات الخاصة.

ومن أمثلة التجارة الإلكترونية لمشروعات الأعمال فيما بينها المتاجرة عبر شبكة الانترنت مباشرة في سلع مثل الصلب والبلاستيك والكيماويا ت كما تشمل أيضا تحالفات بين شركات صناعة السيارات والطيران والفضاء، فيما تعتبر التجارة الدولية النموذج الأمثل لهذا النوع من أعمال التجارة الإلكترونية.

من الأعمال إلى المستهلك: business to consumer: تختصر في (2 C b)*هذا النمط للتجارة الإلكترونية يمثل البيع بالتجزئة في التبادل التجاري العادي

---

[5] - عبد الفتاح بيومي حجازي، مقدمة في التجارة الإلكترونية العربية، دار الفكر الجامعي، 2004، ص: 130.

[6] - عبد الفتاح بيومي حجازي، نفس المرجع،ص: 100.

[7] – د. محمد سعيد أحمد إسماعيل، مرجع سابق، ص: 22 و 23.

* (b 2 b) business to business (من أعمال إلى أعمال)

* (b 2 c) business to consume (من أعمال إلى مستهلك)

وعرف هذا النوع توسع بشكل كبير مع ظهور المراكز التجارية الإفتراضية والأسواق الإلكترونية على شبكة الأنترنت، فتقدم هذه المراكز خدماتها من خلال شبكات الأنترنت، ويتم بطرق مختلفة.

تمتاز هذه المراكز التجارية بجمهورها المختلف من دول العالم، فهي تقوم بعرض تشكيلة واسعة من المنتجات والخدمات لتزيد من عدد الزائرين ومن أمثلتها ذلك المجمع التجاري الإلكتروني الموجود في سريلانكا الذي يعرض مختلف أنواع الشاي والملابس والأحجار الكريمة التي يشتهر بها هذا البلد.

من مستهلك إلى مستهلك: consumer to consumer: تختصر في (C 2 C)* ويتم هذا النوع من التجارة الإلكترونية خلال شبكة الانترنت، وتقوم هذه الفئة من الأفراد بالبيع أو الشراء بشكل مباشر على شبكة الأنترنت, ومن ثم إعادة بيعها إلى مستهلكين الأخرين وهذا يقصد تحقيق الربح ... ومن أمثلة ذلك نذكر مجلة الوسيط الإعلانية التي جازت على شهرة واسعة في مختلف الدول العربية، فقد أنشأت موقعها لها على شبكة الانترنت وأتاحت للأفراد إضافة الإعلانات التجارية التي تتضمن شراء أو بيع أو تبادل للسلع أو المنتجات أو الخدمات مع مستهلكين آخرين، ويستطيع الأفراد البيع أو الشراء من المزادات المفتوحة على الشبكة مباشرة.

من مستهلك إلى أعمال: consumer to business: تختصر في (c 2 b)* ويتمثل هذا النوع من التجارة الإلكترونية بأنه يتم بين مستهلك ووحدة أعمال ويتجسد هذا الشكل في إقدام بعض الأفراد على تقديم خدمات أو معلومات أو منتجات إلى الشركات وغالبا ما يكون هؤلاء الأفراد وسطاء يعرضون خدماتهم عبر مواقع على شبكة الأنترنت، وقد تكون هذه موقع خاصة بهم أو مواقع إعلانية حيث يطلبون باعة ويتفاعلون معهم، ويرمون الصفقات على الخط مباشرة، ويطلق على هؤلاء الأفراد بـــ (الوسيط الإلكتروني).

المطلب الثالث: خصائص التجارة الالكترونية

---

* (C2 C)"Consumer to consumer" (من مستهلك إلى مستهلك)

* (C.2.b) "Consumer to business." (من مستهلك إلى أعمال)

يقصد بها السمات المميزة للتجارة الالكترونية، والتي تجعلها مختلفة عن التجارة التقليدية، ومن أبرز هذه الخصائص:

1) غياب العلاقة المباشرة بين الأطراف المتعاقدة:

إن في التجارة الالكترونية لا يكون فيها مجلس للعقد بالمعنى التقليدي أو مفاوضات جارية للاتفاق على شروط التعاقد، لان البائع يكون في مكان والمشتري قد يبعد عنه بآلاف الأميال، كما قد يختلف التوقيت الزمني بين مكاني المشتري والبائع[8].

قد يغيب العنصر البشري وتتراسل الأجهزة وفقا للبرامج المعدة لها مثل ما قامت به الشركات، حيث تقوم بجرد المخزون من سلعة معينة وتقع أوامر جديدة للشراء للموردين، إذا نقص المخزون عن حد معين تقوم أجهزة الكمبيوتر لديهم باستلام أوامر الشراء وتنفيذها وإرسال فواتير البيع دون تدخل العنصر البشري9

2) الطابع الدولي أو العالمي:

التجارة الالكترونية وبالأخص الوسائط الالكترونية لا تعرف الحدود المكانية، ومنه فإن النشاط التجاري يقدم سلعا أو خدمات على الانترنت لا يحتاج إلى التوجه إلى منطقة جغرافية بعينها، فبمجرد إنشاء موقع تجاري على الانترنت تزود الشركة صاحبة الموقع بإمكانية الوصول إلى الأسواق ومستخدمي شبكة الانترنت عبر العالم كله، ويمكن أيضا إدارة المعاملات التجارية بكفاءة لأي شركة من خلال موقعها أي موقع جغرافي، بالإشارة إلى أن الصفة العالمية للتجارة الالكترونية هي صفة نظرية، وقد لا تطبق على جميع مواقع التجارة الالكترونية.10

3) وجود الوسيط الالكتروني:

---

[8] **Éric A. CAPRIOLI, Loi du 6 août 2004. Commerce à distance sur l'Internet et protection des données à caractère personnel, Revue Communication Commerce électronique n° 2, Février 2005, Etude 7**

[9] – مجموعة من الخبراء: العقود والاتفاقات في التجارة الالكترونية، أوراق ندوة عقود التجارة الالكترونية ومنازعاتها، 2007، ص55.

[10] – د.إبراهيم العيسوي: التجارة الالكترونية، المكتبة الأكاديمية، 2003، ص31.

المقصود به الحاسوب أو الكمبيوتر لدى كل من الطرفين المتعاقدين، والمتصل بشبكة الاتصالات الدولية التي تقوم بنقل التعبير عن الإرادة لكل من الطرفين المتعاقد ينفي نفس الوقت رغم تباعد المكان[11].

لقد تخصصت عدة شركات مثل شركة مايكروسوفت الأمريكية في إعداد برامج متخصصة للإعلان والتسويق، وخدمات البيع وخدمات أخرى، مما أدى لسرعة انجاز الأعمال بأقل تكلفة،وسهل على الشركات والأفراد التحول من النظام التقليدي في المكتب إلى استخدام نظام الكمبيوتر توفيرا لما يمكن من عمليات.12

4) التعامل دون كشف عن هوية المتعاملين مع احتمال تعرض معلومات العملاء أو إساءة الاستخدام عند تقديمها:

قد تعقد صفقة تجارية عبر الانترنت بين طرفين لا يعرف أحدهما الآخر، ولا يملك أي منهما معلومات متعلقة بالآخر، وقد يقدم طرف لآخر معلومات زائفة حيث لا يمكن للطرف الآخر أن يتأكد منها، أو يتعامل معه ببطاقة ائتمان مسروقة أو الوعد بتقديم خدمات ما بعد البيع دون ضمان حقيقي[13].

في حالة ما إذا قدم طرف إلى الطرف الآخر معلومات عن نفسه فقد تتعرض هذه المعلومات للإفشاء أو إساءة الاستخدام لأن صاحبها لا يملك الفرصة للسيطرة على استخدام هذه المعلومات، وهو ما يثير مسالة الخصوصية وسرية المعلومات [14]، ولهذا هناك اجتهادات في هذا الشأن من أجل الحفاظ على الخصوصية وتوفير الأمان والنزاهة في التعاملات التجارية عبر الانترنت15.

---

[11] **Éric A. CAPRIOLI, Loi du 6 août 2004. Commerce à distance sur l'Internet et protection des données à caractère personnel,** Revue **Communication Commerce électronique n° 2, Février 2005, Etude 7**

[12] – مجموعة من الخبراء، المرجع السابق، ص58.

[13] **Éric A. CAPRIOLI, Loi du 6 août 2004. Commerce à distance sur l'Internet et protection des données à caractère personnel.**

[14] **Agathe LEPAGE, Réflexions de droit pénal sur la loi du 6 août 2004 relative à la protection des personnes à l'égard des traitements de données à caractère personnel,** Revue **Droit pénal n° 3, Mars 2005, Etude 5**

[15] – د.إبراهيم العيسوي: المرجع السابق، ص33.

المبحث الثاني: أحكام عقد التجارة الالكتروني

يتساوى عقد التجارة الالكتروني مع بقية العقود التجارية بقيامه على مبدأ الرضا، بحيث يلزم لانعقاده ارتباط الإيجاب بالقبول وتوافقهما على انعقاد العقد، وطبقا للقواعد العامة فان كل من الإيجاب والقبول يعبر عن إرادة من صدر عنه، وهما لفظان مستعملان عرفا لإنشاء العقد.16

يتم إبرام العقد في التجارة الالكترونية بتبادل التعبير عن إرادتين متطابقتين، ويصدر من أحد الطرفين المتعاقدين التعبير في صورة الإيجاب (Offer) ويسمى الموجب (Oferen)، ويتخذ التعبير صورة القبول (Acceptence) من الطرف الآخر ويسمى القابل (Accepter)17.

والتعبير عن الإرادة قد يكون باللفظ أو الكتابة أو بالإشارة المعهودة عرفا، أو المبادلة الفعلية الدالة عن التراضي.

المطلب الأول: الإيجاب الالكتروني

يعرف الإيجاب بأنه تعبير عن إرادة التعاقد يصدر من أحد الأشخاص مفصحا من خلاله عن نيته في إبرام عقد بشروط أساسية محددة، وإذا اقترن الإيجاب بقبول بدون تعديل أو تحفظ انعقد العقد قانونا.18

يعرف التوجيه الأوروبي الخاص بحماية المستهلكين الإيجاب في العقود المبرمة عن بعد بأنه اتصال عن بعد يتضمن كل العناصر اللازمة بحيث يستطيع المرسل إليه أن يقبل التعاقد مباشرة ويستبعد من هذا النطاق مجرد الإعلان[19].

---

[16] – د.نضال إسماعيل برهم: أحكام عقود التجارة الالكترونية، دار الثقافة للنشر والتوزيع، ط2005، المرجع السابق، ص31

[17] - د.محمد سعيد أحمد إسماعيل: أساليب الحماية القانونية لمعاملات التجارة الالكترونية، رسالة دكتوره، ص168

[18] – د.محمد سعيد أحمد إسماعيل: المرجع السابق، ص129.

[19] **Éric A. CAPRIOLI, Loi du 6 août 2004. Commerce à distance sur l'Internet et protection des données à caractère personnel**……..

إن الإيجاب الموجه للتعاقد هو الذي يتوفر على كافة الدلائل التي توحي لإنشاء العقد، ويجب أن يكون مقصود من طرف الموجب حتى تكون له القوة لقبول هذا الإيجاب.

يتعين في الإيجاب أن يكون حازما أي يعبر عن إرادة مصممة وعازمة نهائيا على إبرام العقد إذا ما صادف قبولا، وبالتالي فإنه لا يعد إيجابا مجرد الدعوة إلى التفاوض أو الإعلان حتى ولو تضمن كافة العناصر الرئيسية للعقد.

بناءا على ما تقدم فنا الإيجاب يخضع للإرادة بهدف إقامة علاقة شخصية والسعي من ورائها إلى إجراء عقد،والإيجاب لا يخضع لأي شروط شكلية ولكن يشترط أن يكون محددا وواضحا، يتضمن أساسيات العقد، كتحديد المبيع والثمن، كما يستلزم أيضا أن يتصل الإيجاب بعلم من وجه إليه. 20

نظرا لطبيعة التجارة الالكترونية والفضاء الالكتروني الذي يتم من خلاله، مع إدراجه من الناحية التشريعية ضمن طائفة العقود التي تبرم عن بعد فإن الإيجاب يجب أن يتم تعريفه ضمن هذه الخاصية.

لقد اختلفت بعض الآراء بشأن تحديد الإيجاب، ففي بعض القوانين يرون أن العرض الموجه إلى العالم كله عن طريق الإعلانات لا يعد إيجابا وإنما دعوة إلى التعاقد لأنه يفقد صفة التحديد، ورأى البعض الآخر عكس ذلك منها القانون الفرنسي والانجليزي بأنه من الممكن أن يوجه إلى الجمهور ككل، وأوجه الاختلاف في الرأيين أن الرأي الأول يعلن المنتج عن سلعة في التلفاز أو في أي وسيلة أخرى ويدعو إلى شرائها، ومنه لا يعد هذا العرض إيجابا لأنه غير محدد لشخص معين بذاته أو مجموعة أشخاص.

أما الرأي الثاني يعرض السلعة ويصفها ويحدد مزاياها وثمنها ويؤكد التزامه واستعداده لكل من يرغب في شرائها لإرسالها له وذلك وفقا الشروط المعلنة عنها، ولكنه يتمثل إيجابا صريحا لأنه يعبر عن إرادة صاحبه للتعاقد مع أي شخص.

---

[20] – د.نضال إسماعيل برهم: المرجع السابق، ص34–35.

مما سبق فإن الإيجاب يبقى قائما طوال المدة المحددة ولا يحق للموجب الرجوع فيه، أما إذا لم تحدد المدة فيمكن لصاحبه العدول عن الإيجاب ولكن إذا صدر القبول قبل فلا يحق له الرجوع، لذلك نصت المادة (16) من اتفاقية الأمم المتحدة بخضوع عقود البيع الدولية للبضائع لسنة 1980 حيث نصت:" يجوز الرجوع عن الإيجاب لحين انعقاد العقد إذا وصل الرجوع عن الإيجاب إلى المخاطب قبل أن يكون هذا الأخير قد أرسل قبوله".21

قد ينقضي الإيجاب في حالة الموت (وفاة الموجب)، وقد ذهبت محكمة النقض الفرنسية إلى أن الإيجاب يغدو عديم المفعول بوفاة فاعل الإيجاب، وورثته غير مرتبطين بمجرد إيجاب من أنجبهم، ويفهم أن الإيجاب لا يكون ملزما في حالة تحديد مدة للإيجاب، أما إذا حددت فيبقى الإيجاب قائما وينتقل إلى ورثته، ولا يمكن الرجوع فيه، باستثناء العقود ذات الطابع الشخصي.22

لقد تضمنت العديد من القوانين الجنائية الوضعية عقوبات خاصة في حالة استمالة المستهلكين وحثهم على الشراء عن طريق الإرسال الجبري للعروض الموجهة بالمراسلة دون طلب سابق، ويتم إرسال عروض للسلعة عن طريق البريد العادي أو البريد الالكتروني بشكل مكثف، فبهذا الوصف لا تعد عروضا قانونية باعتبار أن هذه العروض تتضمن نوعا من الإكراه، ويتعرض القائمون عليها للمسألة الجزائية.23

أما بخصوص لغة العقد فقد استوجبت بعض القوانين استعمال اللغة الوطنية في كل العقود24، لكن كما ذكرنا سابقا أن الإيجاب الالكتروني هو إيجاب عابر للقارات أي يمكن أن يتعد الحدود الإقليمية لكل دولة ويعني هذا أنه يخاطب الشعوب متنوعة تتحدث لغات مختلفة، الأمر الذي يعوق إبرام العقد الالكتروني في مثل هذه الحالات، ومثال ذلك ما نصت عليه المادة السادسة من القانون الفرنسي الصادر في أغسطس 1994

---

[21]– نضال إسماعيل برهم: المرجع السابق، ص35– 36.

[22]– نضال إسماعيل برهم، المرجع، نفسه، ص37.

[23]– محمد سعيد أحمد إسماعيل: المرجع السابق، ص141

[24]– نضال إسماعيل برهم، مرجع سابق، ص: 40.

واستلزم استعمال اللغة الفرنسية أو على الأقل الترجمة في التعبير عن الإيجاب في كافة أنواع المعاملات ومنها التجارة الالكترونية.

يلاحظ أن مثل هذه القوانين المحلية تعوق إبرام العقد، ويصعب التعامل بها في التجارة الالكترونية، وهذا ما جاء به التوجيه الأوروبي الصادر في 21 مايو 1992، حيث إذا صدر إيجاب بخصوص بيع عن طريق التليفون أو ما شابه فلا يجوز أن يتوقع شخص تلقي جميع المعلومات بلغته الوطنية بحيث تكون عائقا أمام العقد العابر للحدود.25

يجب الإشارة إلى أن بعض العقود تشترط ما يسمى نطاق التغطية أي تحديد المكان، أي النطاق الجغرافي الذي يغطيه الإيجاب، ومنه فإن العقود لا تنعقد إلا في الحدود الجغرافية التي تحددها الإيجاب، وخلاصة القول أن الإيجاب الالكتروني لا يختلف عن الإيجاب التقليدي لا من حيث التعبير عنه فهو مختلف.

المطلب الثاني: القبول الالكتروني

هو التعبير عن الإرادة لمن قدم إليه الإيجاب في إبرام العقد، ولصحة انعقاد العقد لابد من مطابقة القبول بالإيجاب، إذن فالإيجاب والقبول هما إرادتان لازمتان لإنشاء العقد، ويتساوى في التعبير عن القبول بأن يكون صريحا أو ضمنيا وفق ما نص المشرع الأردني في المادة 93 من القانون المدني، والتي جاء فيها:" التعبير عن الإرادة يكون باللفظ وبالكتابة وبالإشارة المعهودة عرفا ولو من غير الآخرين، وبالمبادلة الفعلية الدالة على التراضي وباتخاذ أي مسلك آخر لا تدع ظروف الحال شكا في دلالته على التراضي.26

نفهم من هذا النص أن القبول باعتباره تعبيرا عن الإرادة ، بحيث يمكن أن تتعدد صور القبول الالكتروني كما في القبول التقليدي، كان يكون طريحا باللفظ أو الكتابة أو

---

[25]–محمد المرسي زهرة: الحماية المدنية للتجارة الالكترونية (العقد الالكتروني– الإثبات الالكتروني– المستهلك)، دار النهضة العربية، الطبعة1، 2007، ص40– 41.

[26]– محمد إبراهيم أبو الهيجاء: عقود التجارة الالكترونية، المرجع السابق، ص48.

إشارة، أو ضمنيا باتخاذ موقف معين بدل بما لا يترك مجالا للشك على التراضي، ولا يختلف كما سبق الذكر القبول الالكتروني في كل ذلك عن القبول العادي.27

يتصور أن آلية التعبير عن القبول الالكتروني "Electronic Acceptance" تتم بواسطة شبكة الانترنت تجد أنها تتأتى بإحدى الطريقتين: إما من خلال موقع العرض نفسه " Web Site" بأن يقوم القابل (المستهلك) بإدخال البيانات الخاصة بالعقد المعروض على الشاشة ودفع ثمن المبيع وذلك بعد نقر على المفتاح الخاص بالقبول (Accept Lok)، أو أن يتم التعبير عن القبول بواسطة البريد E-mail، بأن يقوم القابل بتضمين الرسالة الالكترونية قبوله.28

تؤيد هذه القاعدة التشريعات المقارنة كقانون التجارة الموحد الأمريكي، وكذلك فإن محكمة الاستئناف البريطانية سنة 1995، قد نوهت إلى أن القبول بالسكوت يمكن أن يؤخذ به إذا كان الشخص الذي وجه إليه الإيجاب قد اقترح بأن السكوت سيكون في القبول.

مما سبق فأن القبول لا يكون إلا إذا تم بالشكل المطلوب كان يكون القبول بواسطة البريد الالكتروني أو بإرسال فاكس ...الخ، وفي معظم الأحيان ما يكون المراد من اشتراط طريقة محددة للقبول هو تأكيد القبول لحماية المستهلك في حالة الخطأ [29] بالنقر على الأيقونة المخصصة للقبول بدون قصد، وتشترط بعض التشريعات الخاصة بحماية المستهلك الالكتروني تأكيد القبول وفي ذلك حماية للبائع أيضا، وذلك حتى لا يستطيع المشتري الطعن في العقد بدلالة على أن قبوله كان قد تم بطريق الخطأ.30

قد يثور التساؤل حول مدى التزام الموجب بالقبول على الرغم من عدم عمله ببعض الشروط التعاقدية، وللإجابة عن هذا التساؤل وعند اعتبار عقد التجارة الالكترونية عقد إذعان، فإن مثل هذا الشرط يعتبر شرطا تعسفيا بحيث يمكن إلغاؤه واعتباره كأن لم يكن توافقا مع المادة 204 من القانون المدني الأردني والتي تنص

---

[27]– محمد المرسي زهرة: نفسه، ص43.

[28]– محمد إبراهيم أبو الهيجاء: المرجع السابق، ص48.

[29] **Agathe LEPAGE, Réflexions de droit pénal sur la loi du 6 août 2004 relative à la protection des personnes à l'égard des traitements de données à caractère personnel**

[30]– محمد سعيد أحمد إسماعيل: المرجع السابق، ص146– 147.

على: "إذا تم العقد بطريق الإذعان وكان قد تضمن شروط تعسفية جاز للمحكمة أن تعدل هذه الشروط أو أن تعفي الطرف المذعن منها وفقا لما تقفي به العدالة، ويقع باطلا كل اتفاق على خلاف ذلك".

بما أن القبول يضبط بشرط شكلي نزولا عند مبدأ الرضائية بحيث يمكن أن يكون بأي صورة صريحا أو ضمنيا، كتابة أو شفاهة، أو عن طريق آلة كاتبة إلى آخره، غير أن هذه الحرية للمتعادين في التعبير عن إرادتهما يحد منها ما يتطلبه القانون في شأن إثبات العقد.

العقود الالكترونية من العقود الرضائية التي لا تتطلب شكلا معينا للقبول، بحيث يمكن ابتكار وسائل معينة للتعبير عن القبول، مثل استخدام وثيقة أمر بالشراء يتعين على المستهلك أن يحررها على جهازه حتى تنتقل إلى موقع البائع، بحيث يكون القبول مؤكدا وجازما.31

عند المقارنة بين النظريات السابقة نلاحظ أن نظرية العلم بالقبول هي النظرية الأحسن على اعتبار أن الموجب طرف من أطراف العقد ومن الأولى أن يعلم بقبول القابل حتى يتسنى البدء في تنفيذ العقد، إلا أن البعض يرى أن نظرية العلم بالقبول قد تعطي فرصة للموجب للتلاعب، بحيث يتعهد عدم العلم أو يردعه إن كان ذلك في صالحه، وللرد على ذلك نقول أن البائع أعطى رخصة وضع شروط في عرضه، بحيث يحتفظ من خلالها لنفسه بإمكانية تعديل السعر أو رفض المبيع، أما بشأن تحديد مكان وزمان التعاقد في العقود الالكترونية فإننا سنتحدث عن التعاقدات التي تجري عن طريق الهاتف والمراسلة البريدية ونحاول معرفة موقع المراسلات الالكترونية التي تجري عن طريق الانترنت[32].

إن إبرام العقد على الهاتف أو عبر البريد العادي يفهم من أنها تتم بين غائبين أي يجمعهما مجلس واحد، لكن نقطة اختلافهما في تحديد لحظة التعاقد، حيث يتم تحديد

---

[31]– نضال إسماعيل برهم: المرجع السابق، ص45.

[32] **Éric A. CAPRIOLI, Loi du 6 août 2004. " Commerce à distance sur l'Internet et protection des données à caractère personnel** "……

وقت التعاقد في الهاتف كأنه يحصل بين حاضرين، أما في المراسلة قد يكون هناك فاصل بين صدور القبول والعلم.

إن الرسائل الالكترونية التي تجري عن طريق الانترنت مع الهاتف يتشابهان في أنهما يتمان بشكل لحظي، ولأن كلاهما نظام تفاعلي، لكن يختلفان من حيث أنه قد تفصل بين إرسال الرسائل الالكترونية واستلامها فاصل بمعنى الرسالة لا تنتقل مباشرة وإنما يتدخل وسيط بين المرسل والمرسل إليه، ويتمثل هذا الوسيط في مورد الخدمة سواء للمرسل أو المستهلك.33

أما بالنسبة للتعاقدات التي تتم عن طريق الانترنت يفرق في ذلك بين التي تعقد عن طريق البريد الالكتروني وتلك التي تعقد عن طريق شبكة الويب.

أخيرا يجب ابتكار وسائل تؤدي إلى قبول مدروس غير انفعالي صادر عن قناعة حقيقية ورغبة أكيدة في التعاقد، كما يجب أن يعطي هذا القبول المفاعيل القانونية بحيث يكون بالإمكان إثباته حتى يكون له وجود قانوني فعلي.34

المطلب الثالث: زمان ومكان انعقاد العقد

زمان انعقاد العقد: لا شك أن تحديد لحظة القبول لها أهمية كبيرة بمعنى أنها اللحظة التي ينعقد فيها العقد، فالعقد لا ينعقد بتلاقي الإيجاب والقبول، ولا يتحقق ذلك إلا من وقت قبول الإيجاب دون زيادة أو نقصان، لكن الأمور لا تسير بمثل هذه السهولة في طائفة العقود التي تبرم عن بعد، والتي يدخل من ضمنها العقد الالكتروني، إذ ينعقد العقد دون حضور مادي بين الأطراف زمن هنا يفترض أن يكون هناك فارق زمني بين صدور القبول والعلم به، ومن هنا يثور المشكل حول اللحظة التي ينعقد العقد وقتها[35].

إن هذه المشكلة عامة في الحقيقة لا تتعلق بالعقد الالكتروني فقط، فقد تتعلق بالمراسلة بصفة عامة، وتطرق الفقه التقليدي إلى أربع نظريات في هذا الخصوص

---

[33]– المرجع نفسه، ص60 وما بعدها

[34]– نضال إسماعيل برهم: المرجع السابق، ص46.

[35] **Éric A. CAPRIOLI, Loi du 6 août 2004. Commerce à distance sur l'Internet et protection des données à caractère personnel**……

لتحديد لحظة انعقاد العقد، وهي: نظرية إعلان القبول ويرى أنصارها أن العقد ينعقد بمجرد إعلان الموجه إليه الإيجاب قبوله، والنظرية الثانية هي تصدير القبول بحيث ينعقد العقد في نظر أنصارهم من الوقت الذي يرسل فيها القابل قبوله، بحيث لم يعد يستطيع استرجاعه، ونظرية استلام القبول ويرى أنصارهم أن العقد ينعقد بوصول القبول إلى الموجب، وأخيرا نظرية العلم بالقبول حيث يرون أن العقد لا ينعقد إلا من لحظة علم الموجب بالقبول.36

يعتبر البريد الالكتروني من أكثر الطرق التقنية استخداما للتعاقدات في التجارة الالكترونية باعتبارها وسيلة سهلة للتواصل عبر الانترنت، ولذلك يمكن القول أن البريد الالكتروني ما هو إلا وسيلة لإرسال واستقبال الرسائل والمعلومات عموما.

قد يكون الموقع الالكتروني يطرح إيجابا ولا يقدم دعوى للتعاقد، في هذه الحالة يكون الاختلاف في تحديد لحظة القبول وانعقاد العقد وما ينبني على ذلك من تحديد لمكان إبرام العقد، ومنه يكون الحل لهذه المسالة بترك تحديد وقت انعقاد العقد واستلام القبول لإرادة المتعاقدين المسبقة على التعاقد، فإذا كان الموقع الالكتروني يقوم بعرض الإيجاب فعليه أن يوضح للمستهلكين الكيفية التي سيتلقى فيها القبول مع بيان الوقت الذي يعتبر معه العقد إذا انعقد، أما إذا كان الموقع يقوم بعرض دعوة فقط فعليه أن يبين للموجهين الآلية التي يستقبل فيها الإيجاب وإصدار القبول حتى يكون الموجب على علم في تحديد اللحظة التي يتم فيها إبرام العقد[37].

لقد ذهب قانون الأونستيرال بشأن التجارة الالكترونية في صدد تحديده لوقت استلام رسالة البيانات على أنه ما لم يتفق المنشئ والمرسل إليه على غير ذلك فانه يتحدد وقت استلام رسالة البيانات على النحو التالي.

من خلال النص لم يتم تحديد وقت القبول نصا واضحا، إلا انه ترك لأطراف العلاقة حرية وقت الاستلام، هذا ما يتماشى مع طبيعة التجارة الالكترونية وانتشارها العالمي.38

---

[36] – محمد المرسي زهرة: المرجع السابق، ص48– 49.

[37] **Éric A. CAPRIOLI, Loi du 6 août 2004. Commerce à distance sur l'Internet et protection des données à caractère personnel**

[38] – محمد إبراهيم أبو الهيجاء: المرجع السابق، ص56.

ذهب بعض من الفقه في شأن تحديد زمن التعاقد في العقود الالكترونية إلى التمييز بين التعاقد الذي يقع بين حاضرين أو غائبين، فإن كان التعاقد يتم بالفاكس يرى البعض إلى انه تعاقد بين غائبين لأن المتعاقدين يفصل بينهما مدة من الزمن، أما إذا كان عن طريق التلكس فإنه يعد تعاقدا بين حاضرين حيث يكون الاتصال مباشر وتوافق الإيجاب والقبول لا يفصل بينهما مدة زمنية.[39]

أما بالنسبة للتعاقدات التي تحدث عن طريق الانترنت فيوجد اختلاف بين التي تعقد عن طريق البريد الالكتروني والتي تعقد عن طريق شبكة الويب.

إن من أكثر الطرق استخداما لإبرام عقود التجارة الالكترونية هو البريد الالكتروني كونه وسيلة سهلة للتواصل عبر الانترنت، ويمكن من خلاله استخدام شبكة الانترنت كمكيف للبريد يرسل بها الرسائل إلى أي شخص لديه بريد الكتروني، وبشأن تحديد زمان انعقاد العقد الالكتروني في البريد الالكتروني يدور التساؤل حول النظريات الثلاثة فقط تتحدد بناءا عليها لحظة انعقاد العقد، نظرية القبول، نظرية استلام القبول، ونظرية العلم بالقبول، وهنا يتضاءل الفارق بين لحظة استلام القبول ولحظة العلم به.

عادة ما يطلع الموجب على القبول بمجرد وصول البريد الالكتروني تسلما له، ولا يطلع على البريد الالكتروني إلا بعد لحظة زمنية قد تطول، لهذا هناك صعوبات في تحديد لحظة انعقاد العقد الذي يتم عبر البريد الالكتروني باعتبار وصول الرسالة الالكترونية دليلا على العلم بها وكيف يثبت الموجب عدم علمه بالرسالة رغم وصولها.[40]

بالنسبة لتحديد زمان التعاقد على شبكة الويب فان العقود التي تنعقد من خلال هذه الشبكة تكون من لحظة النقر على أيقونة القبول، حيث يجد نفسه أمام العقد النموذجي الموضوع في شبكة الويب والتي تتضمن شروط العقد المراد إبرامه.

يحل القبول في اللحظة التي يضغط فيها القابل على أيقونة القبول لذلك عقود الويب تنعقد لحظة نقر الموجه إليه الإيجاب على الأيقونة ما لم يكن هناك عطل فني،

---

[39] – نضال إسماعيل برهم: المرجع السابق، ص62.

[40] – محمد المرسي زهرة: المرجع السابق، ص53.

والأصل أن العقد ينعقد من لحظة وصول القبول إلى الموجب باعتبار أن وصول القبول قرينة على علم الموجب به ما لم يثبت عكس ذلك.41

مكان انعقاد العقد: يحضى مكان انعقاد العقد الالكتروني بأهمية خاصة من حيث تحديد المحكمة المختصة بنظر أي نزاع يتعلق به، ومن حيث تحديد القانون الواجب التطبيق إذا ما اتخذ العقد الطابع الدولي.

قد تركت التوجيهات الأوروبية الحرية لكل دولة في تحديد مكان انعقاد العقد إلا أن قانون الأونستيرال النموذجي حسم ذلك في تحديده لزمان استلام رسالة البيانات، فإذا لم تتفق الأطراف المتعاقدة على مكان إبرام العقد فان العقد يكون قد انعقد في المكان الذي يقع فيه عمل المرسل إليه، وفي حالة ما إذا تعددت المواقع فإنه يستند لموقع العمل الأكثر صلة بموضوع العقد، أما إذا انعدم مقر العمل يتم الرجوع لمحل إقامته المعتاد.

يترتب على اللحظة التي يعتبر فيها أن العقد قد انعقد هي ذاتها التي تحدد مكان انعقاده، وهذه اللحظة هي التي يعلم فيها الموجه بالقبول، فالمكان الذي يعلم فيه الموجه بقبول الإيجاب هو مكان انعقاد العقد. 42

لقد ذهب قانون الأونستيرال بهدف ازدهار التجارة الالكترونية من خلال التشريعات الوطنية باعتماد مقر عمل الموجب كمكان لإبرام العقد الالكتروني، وانعقاده في اللحظة التي يتسلم فيها القبول ما لم يتفق طرفا العقد على خلاف ذلك.

المطلب الرابع: صحة التراضي

بظهور شبكة الانترنت والعقود الالكترونية التي تبرم خلالها أخذ شكل التعبير عن الإرادة شكلا مختلفا، حيث تتم عبر قنوات فضائية في شكل رسائل بيانات، هذا ما أشارت إليه لجنة الأمم المتحدة للقانون التجاري، لذلك يشترط لصحة التراضي أن تصدر عن أهلية كاملة دون وجوب عيب بالنسبة لأهلية التعاقد.

---

[41]– محمد المرسي زهرة نفسه، ص54.

[42]– محمد إبراهيم أبو الهيجاء: المرجع السابق، ص57.

يخضع العقد الالكتروني للقواعد العامة للأهلية وعيوب الإرادة وتتضاءل هذه الأخيرة في الدول التي نظمت قواعد خاصة لحماية المستهلك الالكتروني، إذ يجوز للمستهلك الالكتروني التخلي عن العقد دون إبداء عيوب مبررات، وفي بعض الأحيان تبقى له مصلحة في إثبات توفر أحد عيوب الإرادة، لأن هذه الدول التي أعطت حماية للمستهلك الالكتروني خولت له ما يسمى بخيار الرجوع خلال مدة زمنية قصيرة، فإذا فسخ العقد بسبب التغرير فإنه يخول للمستهلك الحق في طلب تعويض إضافي على أساس المسؤولية التقصيرية.43

يتم الإعلام بالعدول بجميع الوسائل المنصوص عليها في العقد ويتضمن إرجاع المبلغ المدفوع إلى المستهلك في أجل عشرة أيام عملا من تاريخ إرجاع البضاعة أو العدول عن الخدمة، ويتحمل المستهلك المصاريف الناجمة عن إرجاع البضاعة.

يحتاج التاجر إلى التحقق من أهلية المتعاقد لأنه قد يقع ضحية خداع من قاصر يستعمل بطاقة مصرفية لوالده أو احد أقاربه مثلا ويستعملها في التعاقد فهل يجوز طلب القاصر بفسخ العقد لنقص أهليته؟44

يستطيع البائع حسن النية في هذه الحالة التمسك لأنه توفر في القاصر مظهر صاحب البطاقة وبالتالي يكون القاصر مسؤولا مسؤولية تقصيرية ويستطيع البائع الرجوع إلى القاصر، ويتضح أن ناقص الأهلية يمكنه رغم ارتكابه طرق احتيالية فسخ العقد، ويستطيع المتعاقد معه بالمقابل المطالبة بالتعويض عن الأضرار التي أصابته استنادا إلى قواعد المسؤولية التقصيرية.45

يمكن لحل هذه المشكلة أي أهلية المتعاقدين اللجوء إلى ما يسمى سلطات الإشهار والتي هي عبارة عن طرف ثالث ينظم العلاقة بين الأطراف، ويحدد هوية

---

[43]-محمد المرسي زهرة: المرجع السابق، ص56.

[44]–نضال إسماعيل برهم: المرجع السابق، ص48.

[45]–محمد المرسي زهرة: نفسه، ص57.

الطرفين وأهليتهما القانونية عن طريق إصدار شهادات تثبت حقائق معينة متعلقة بالتعاقد الذي يتم عبر شبكة الانترنت.46

المبحث الثالث: إشكالات التجارة الإلكترونية

حاولنا في هذا المبحث دراسة إشكالات التجارة الإلكترونية .فقسمناه إلى ثلاثة مطالب: المطلب الأول هو إختراع مواقع التجارة الإلكترونية و إتلافها. المطلب الثاني هو مشكلة أداء الوفاء . المطلب الثالث هو مشكلة تنفيذ الإلتزام الإلكتروني.

المطلب الأول: اختراق مواقع التجارة الإلكترونية وإتلافها أو تدميرها

عند تعريف التجارة الإلكترونية انتهينا إلى أنها عبارة عن معلومات أو بيانات في إطار قانوني معين، وتنساب عبر وسط معلوماتي، أو نظام معالجة بيانات وكل هذه المعلومات والبيانات يسهل اختراقها أو التلاعب فيها، طالما أمكن اختراق النظام المعلوماتي ذاته، وذلك أمر ممكن بطرق عديدة.47

وإن كل شخص يتولى تقديم خدمة على الشبكة يجب أن يحوز إسما مرتبط بالنشاط الذي يمارسه، على نحو يستطيع كل مشترك أو باحث الوصول إلى هذه الخدمة من خلال ذلك اسم الذي يعد بمثابة دليل على وجود الخدمة وموقعها على الشبكة وهذا ما يسمى باسم الدومين وكل من المواقع واسم الدومين والبرامج والمعلومات المعروضة على الشكبة تعتبر بمثابة عمل أدبي يتمتع بالحماية القانونية لحق المؤلف متى توافر بشأنها صفة الابتكار[48].

فالموقع يتم تصميمه وفقا لنموذج يتفق وطبيعته والوظيفة المطلوبة منه تحقيقها ويعبر هذا النموذج عن موضوع الموقع ومكانه. والإذن الممنوح له، هذا بالإضافة إلى

---

[46]–نضال إسماعيل برهم: نفسه، ص49.

[2]- عبد الفتاح بيومي حجازي، التجارة الإلكترونية وحمايتها القانونية، دار الفكر الجامعي، 2004، ص78.

[48] **Éric A. CAPRIOLI, Mesures techniques de protection et d'information des droits d'auteur, Revue Revue Communication Commerce électronique n° 11, Novembre 2006, Etude 30**

السمة الخاصة به التي يضفيها عليه مصممة من خلال رسومات أو لغة فنية أو بيانات مميزة خاصة به، إن الموقع عمل مبتكر يخطى بحماية قانون الملكية الفنية والأدبية.49

ومما سبق ذكره فهدف التجارة الإلكترونية هو الحماية أي المحافظة على سرية المعلومات، فالمشاكل التي تنجم مثلا: أي عمل تجاري لديه من المعلومات التي إذا أفشيت أو سرقت فسوف يؤثر سلبا. وبدرجة كبيرة على نشاطها التجاري.

ومن الأمور التي تهدد التجارة الإلكتروني ة هو إفشاء سرية هذه المعلومات.و الأمثلة على التهديدات التي تواجه التجارة الإلكترونية كثيرة ومتزايدة ولذلك يتعين على المؤسسات التجاريةِ التي دخلت حقل هذه التجارة تأمين مواقعها، ويمكن حصر حديث الموضوع كما يلي:

الفرع الأول: اختراق المواقع (انتهاك نظام الحماية والسرية)

إن أهم صور التعدي على الموقع هي محاولة اختراقه بغية الحصول على المعلومات الاقتصادية والشخصية والفنية ويقوم بذلك ما يطلق عليهم القراصنةHackers سواء كانو ا هواة أو محترفين 50. ويستطيع قراصنة الحاسب التوصل إلى المعلومات وذلك راجع إلى أن التطور المذهل للحاسب الآلي ونظمه ووسائل الاتصال.

يصاحبه تقدم أعظم في الجريمة المعلوماتية، ويسهل ارتكابها، سيما وأن مرتكبي هذه الجرائم ليس مجرمين عاديين بل هم خبراء الكمبيوتر سواء كانوا محترفين أم هواة.51

كذلك قد يتم هذا الإختراق عن طريق أشخاص آخرين وهم المهنيون المتدخلون في خدمة الأنترنت أي الوسطاء في تقديم الخدمات مثل: متعهد الوصول أو الإيواء أو

49– محمد حسين منصور، المسؤولية الإلكترونية، دار الجامعة الجديدة، 2003 ص: 255 و 256.

50- محمد حسين منصور، مرجع سابق، ص، 256.

51– عبد الفتاح بيومي حجازي، مرجع سابق، ص: 80.

الخدمات، ناقل أو مورد المعلومات ويشير مثل هذا الإختراق كل من المسؤولية المدنية والجنائية[52].

والحقيقة أن الإشارة إلى هؤلاء الأشخاص لم يكن المقصود منه حصر المسؤولين عن مهاجمة مواقع التجارة الإلكترونية على الشبكة كذلك تثور مسؤولية المستخدم العادي للانترنت حتى دخل إلى الموقع دون سداد الرسوم المقدرة –إذا كان هناك رسوما– أو تجاوز في بقائه المدة المحددة له، أو كان الموقع مشفرا أو مرمزا هذا ويحضر الدخول إليه وقد أدى التطور المذهل للحاسب الآلي ونظمه وسبل الإتصال إلى تعدد الطرق التي يمكن من خلالها إلتقاط المعلومات المتعلقة بالتجارة الإلكترونية فهناك مثلا توصيل الخطوط التي ترسل إشارات إلكترونية مبكرة بالمعلومات المطلوبة. كذلك يمكن التقاط الذبذبات، والصادرة عن طريق هوائي مستقبل لإرسال القمر الصناعي حتى كانت المعلومات تثبت عن طريقه أو التوصيل المباشر على خط تليفوني عن طريق وضع مراكز تصنت أو إلتقاط الإشاعات الصادرة عن الجهاز المعلوماتي، أوفك شفرة المعلومات أو تسرب البيانات الرئيسية والرموز الخاصة ببرامج الشبكة.53

من معوقات أو صعوبات التي تواجه العالم بسبب هذه الظاهرة وهي "الإختراق" لمواقع التجارة الإلكترونية فثمة معوقات تحول دون التعاون الدولي الأمثل لمحاربة هذه الظاهرة وتتمثل في[54]:

الطفرات التي يشهدها قطاع التكنولوجية مثلا السرعة التي يتم بها إنتاجه الكمي والنوعي.

عدم وجود قانون دولي يجرم هذا النوع من الجرائم.

عدم وجود السلطة القضائية المختصة في مثل هذه الجرائم ذلك أن الجريمة الإلكترونية (المعلوماتية) لها طبيعة خاصة.

---

[52] **Éric A. CAPRIOLI, Mesures techniques de protection et d'information des droits d'auteur,**

[53] - محمد حسين منصور، نفس المرجع، ص: 257.

[54] **Éric A. CAPRIOLI, Mesures techniques de protection et d'information des droits d'auteur,**

عدم وجود شبكة دولية لتبادل المعلومات الأمنية كما في شبكة يورب بول آتي تعمل في إطار الشرطة الدولية.

اختلاف في الشكل والحكم الذي تتخذه تلك الجرائم التي تعددت مابين سرقة معلومات وسرقة برامج وسرقة أرقام بطاقات ائتمانية.

زيادة عدد المشتركين وتنوعهم وصعوبة التعرف والسيطرة عليهم.

عدم وجود تنسيق دولي وسلطة مركزية تهمين على نشاط الشبكة والتحكم فيها.[55]

الفرع الثاني: إتلاف المواقع وتدميرها

لعل أخطر صور التعدي على المواقع تتمثل في محاولات إتلافها وتدميرها عن طريق استخدام ما يسمى بالفيروس المعلوماتي.[56]

الفيروس اصطلاحا دخل حديثا إلى مجال صناعة الحاسب الآلي ليقوم ببعض الأساليب الغادرة والماكرة والتي يمكن عن طريقها غزو الحاسب، وببساطة شديدة. فإن الفيروسا هو برنامج للحاسوب الآلي مثل أي برنامج آخر، لكنه يهدف إلى أحداث أكبر ضرر بنظام الحاسب وله القدرة على ربط نفسه بالبرامج الأخرى، وكذلك إعادة إنشاء نفسه حتى يبدو كأنه يتكاثر ويتولد ذاتيا، ويقوم بالانتشار بين برامج الحاسب المختلفة وبين المواقع المختلفة في الذاكرة.

من خصائص الفيروس أنه معدي، أي هو مجموعة من التعليمات والأوامر المتعارضة والممنوعة وغير المشروعة. وكذلك فإن الفيروسات تظهر بدون مقدمات وبدون توقعات فقد يكون في شكل صوت مرتفع يظهره الحاسوب.

---

[55] - عبد الفتاح بيومي حجازي، المرجع السابق، ص: 85.

[56] - محمد حسين المنصور،المرجع السابق، ص: 258.

في ساعة معينة كالساعة الخامسة مثلا كما أن الفيروسا ت لا تسبب إزعاجا فقط ولكنها مكلفة ماليا، ولذلك فإن الفيروس المعلوماتي وثيق الصلة بالجريمة المعلوماتية إذ قد يؤدي لتلف المعلومات أو تغير مضمونها.

وتتلخص وسائل عدوى الفيروس في ثلاث طرق. كما حددها إتحاد الفيروس الكمبيوتر computer virus Industry association ويشار إليه اختصارا بـــ: C. V. I. A وذلك بولاية كاليفورنيا الأمريكية. فقد يكون من خلال نقل الأجهزة أو من خلال شبكات الاتصال، وأخيرا من قرص ليس مصابا من مصدر خارجي.57

وهناك أنواع كثيرة للفيروسات يصعب حصرها بعضها يعيب الملفات وبعضها الآخر يعيب قطاع التحميل ومنها "الكرة المرتدة، مايكل أنجلو، المخ، أول أبريل، الدورة المعلوماتية،... إلخ. فهذه الفيروسات تضرب أنظمة الحاسب الآلي، ومن ثم تؤدي وبشدة على التعاملات الإلكترونية ومنها التجارة عن بعد، لذلك فهي في تطور مستمر، وذلك ناتج للتطور المعلوماتي في نظام الحاسب الآلي وتقدم التجارة الإلكترونية عبر الأنترنت.58

مما سبق رأينا سبل إختراق الحاسب الآلي، وشبكات الانترنت وإتلاف مواقعها عن طريق الفيروسات، وذلك لأن هذه التجارة عبارة عن مراكز تسويق إفتراضية على الشبكة تتداول فيها بيانات بائع أو منتج لسلعة أو خدمة ومستهلك أو مشترى هذه الخدمة أو السلعة، لذلك فإن مستقبل التجارة الإلكترونية مرهون بمدى تقدم سبل الحماية لمواقع التجارة من الإختلاف أو حمايتها من الفيروس ضد الإتلاف أو التدمير، كما أن الشركات التجارية التي تعتمد على هذه التجارة في تسويق سلعها وخدماتها تنفق الكثير من أجل حماية هذه المواقع ضد محاولات الاختراق أو التدمير[59].

وذلك لأن المساس بسلامة مواقع التجارة الإلكترونية تعيش نوعا من عدم توفر الأمن المعلوماتي من جهة المستهلك وأيضا التاجر مما يؤدي كيلهما إلى الإنسحاب من السو ق

---

[57]- عبد الفتاح بيومي حجازي، مرجع سابق، ص: 90.

[58]- نفس المرجع، ص: 94.

[59] **Christophe CARON, Conditions de l'action en contrefaçon dirigée contre une oeuvre de collaboration Communication,** Revue **Commerce électronique n° 2, Février 2007, comm. 19**

الإلكتروني والعودة إلى التعامل في السوق التقليدية، ولهذا لا غرابة أن تجد الشركات الكبرى تنفق الملايين لتطوير سبل الدعاية والحماية لتجارتها الإلكترونية، وهذا من أجل حصد عدد كبير من المستهلكين وذلك من خلال توفير الأمن على الشبكة وهو ما يعني زيادة عدد المستهلكين ومن تم زيادة الأرباح.60

التعدي على الموقع (المحاكاة والاختلاس والتضليل):

كما سبق ذكر فإن الموقع هو تصميم يعتبر بمثابة عمل أدبي يتمتع بالحماية الفكرية والأدبية، ومنه لا يجوز التعدي عليه بالتقليد، أو الاقتباس أو الفسخ بالمخالفة لذلك القانون، فكثير ما تقع مشاكل، تقليد بيانات وإعادة نسخها على أي موقع آخر مما يثور قضايا هي التشابه بين المواقع فيما يتعلق بالشكل و المضمون وأسلوب عرض الخدمات، ولعل الصورة البارزة هي الإختلاس أو الاقتباس وإعادة عرض بيانات الموقع دون إشارة إلى الموقع الأصلي أو التضليل بالإيحاء بأن ذلك المضمون وكأنه خاص بالموقع العارض.

إذا كانت هناك فرصة الإستفادة من الشبكة، فيجب إخطار واستئذان صاحب الموقع الأصلي، ومنه فعملية الإختلاس أو الإقباس يعد سلوك غير أمين يتصف بالتطفل أي الإستلاء على عمل وجهود الآخرين، ومنه فيعتبر الموقع والمضمونة، أمر يتصل بعنصر الإبتكار، وهذا يستند إلى حق الملكية الذهنية مما يتطلب إضفاء عليه الحماية القانونية عليهما.61

المطلب الثاني: أداء الوفاء "بطاقات الائتمان النقود الإلكترونية"

الفرع الأول: تعريف الوفاء الإلكتروني

وهو وفاء بالتزام نقدي بوسيلة إلكترونية مثل الشبكات الإلكترونية والكمبيالة الإلكترونية وبطاقات الدفع والممغنطة.62

---

[60]- عبد الفتاح بيومي حجازي، المرجع السابق، ص: 104.

[61]- محمد حسين منصور، المرجع السابق، ص. 258.

[62] - هدى حامد قشقوش، الحماية الجنائية للتجارة الإلكترونية عبر الإنترنت، دار النهضة العربية، ص: 94.

إن من أسباب ظهور التجارة الإلكترونية هو التقدم العلمي في مجال الاتصال والمعلومات وخاصة في مجال الإنترنت، مما أدى إلى تسهيل عملية دفع النقود وظهور فكرة جديدة هي الدفع الإلكتروني الذي يتم خلال قنوات الاتصال الإلكتروني بين حاسب آلي وإنترنت، ومن المنطقي أن استعمال النقود الإلكترونية يؤدي إلى سرعة وسهولة تسوية المدفوعات الأمر الذي يؤدي إلى توسع في التبادل التجاري.[63]

وتتم أعمال الصرفة الإلكترونية عن طريق بطاقات الدفع الإلكتروني أو بطاقة الائتمان وهي بطاقة مستطيلة من بلاستيك تحمل اسم مؤسسة المصدر لها، شعارها. وتوقيع حاملها، بشكل بارز على وجه البطاقة ورقم حسابه، وتاريخ انتهاء صلاحيتها، وبموجب هذه البطاقة يمكن لحاملها سحب المبالغ النقدية من ماكينات سحب النقود الخاصة بالبنوك، أو أن يقدمها كأداة وفاء للسلع والخدمات أو قد تكون أداة للائتمان.[64]

ويستخدم الحامل هذه البطاقة من أجل الوفاء بالتزاماته بدلا من الدفع الفوري بالنقد، ولابد أن يكون الحامل عميلا لأحد البنوك، وتؤمن مؤسسة الإصدار السهولة في إسيتفاء المدفوعات عن طريق الاقتطاع الشهري من حساب العميل. أو قد يقدم العميل إحدى ضمانات شخصية وعينية، وتصدر البطاقة في حدود السقف مالي معين لا يجوز للعميل تجاوزه، ويوجد من البطاقة التي تستخدم حدود الدولة التي تصدر فيها ولا يجوز استعمالها خارجا ومنها ما هو عالمي.

وتستعمل البطاقة كوسيلة وفاء لحاملها من خدمات أو بضاعة لدى أحد المحلات التجارية التي تضع إشارة معينة تفيد قبول البطاقة كوسيلة وفاء، ومنه يقوم المحاسب الآلي بالتأكد من صلاحية هذه البطاقة من حيث تاريخ سريانها، وعدم كونها من البطاقات الموقوف التعامل بها لأي سبب، ومنه يصدر البائع إيصالا. "إيصال بيع " "sales voucher" من ثلاث نسخ لا تقبل البطاقة، إن تم تجاوز السقف الائتماني في حدود الجزء الذي يتم فيه التجاوز.

---

[63]- عبد الفتاح بيومي حجازي، المرجع السابق، ص: 106.

[64]- نضال إسماعيل براهم، أحكام عقود التجارة الإلكترونية، دار الثقافة للنشر والتوزيع، عمان،2004، ص: 123.

إن التزام التاجر بشروط والتعليمات استخدام البطاقة، فإنه يكتسب حقا مباشرا في مواجهة البنك العميل سواء كان هناك رصيد أم لم يوجد، فالبنك هو ملزم بالدفع للتاجر متى التزم بالتعليمات وشروط استخدام البطاقة الصادرة إليه.

التزام البنك مصدر البطاقة في مواجهة التاجر هو التزام مباشر ومستقل عن العلامة بين البنك مصدر البطاقة وحاملها.

لا يجوز للحامل البطاقة الامتناع عن الوفاء مصدر البطاقة إلى التاجر.

وأخيرا يمكن القول أطراف العملية المصرفية التي تتم عن طريق هذه البطاقات هم بنك العميل حامل البطاقة، حامل البطاقة، والتاجر وبنك التاجر، كما تتضمن البطاقات بيانات أخرى تتعلق بالصورة المجسمة ثلاثي ة الأبعاد، وهو مايطلق عليها (الهولوجرام) وتتضمن كذلك شريط التوقيع، أو رقم التميز الشخصي.65

الفرع الثاني: أنواع بطاقات الاعتماد: (أنواع الدفع الإلكتروني)

إن ظهور التجارة الإلكترونية التي تتم عن بعد، أدى إلى ظهور مشكلة الوفاء والبحث إلى سبل تسوية المعاملات، ونظرا إلى تعدد أنواع وسائل الدفع الإلكتروني ونتعرض لأهم أنواعها:

أ) التحويل الإلكتروني: وتتم عن طريق تحويل مبلغ معين من النقود من حساب المدين إلى حساب الدائن، ويقوم بهذه عملية غالبا بنك.66

ب) البطاقات البنكية (النقود البلاستيكية): وهناك عدة أنواع من هذه البطاقات لعل أهمها:

1. **بطاقات الائتمان (credit card):** وهي بطاقات تصدر بوساطة مؤسسة مالية باسم أحد الأشخاص، وهذه البطاقة تحول لصاحبها (حاملها) الحصول على تسهيل ائتماني من مصدرها. وحيث يستطيع استعمالها للحصول على سلع وخدمات، على أن يتولى

---

65 - عبد الفتاح بيومي حجازي، مرجع السابق ص: 109-110.

66 - محمد حسين منصور، مرجع السابق، ص: 124.

البنك أي مصدر بالدفع، ثم يقوم الحامل بسداد دفعه للبنك مع الفوائد المتفق عليه، ولا تمنح البنوك هذه البطاقات إلا بعد تأكد من المركز المالي للعميل والحصول على ضمانات عينية أو شخصية كافية.

2. **بطاقات السحب الآلي (cash card):** هذا النوع من البطاقات تقدم تسهيلا للعملاء، وتوفير احتياجاتهم من النقود، ويمكن العميل بمقتضاها سحب مبالغ نقدية حتى حسابه بحد أقصى متفق عليه مع البنك.

3. **بطاقة ضمان الشيكات (cheque gauranter card):** يتعهد بها البنك بسداد الشبكات التي يحررها العميل بشروط معينة بمعنى أن يحرر شيكا لأحد التجار، بحيث يعطي ضمانا بأن شيك، سوف يصرف في موعده وإن لم ين هناك رصيد، حيث يضمن البنك مصدر البطاقة ذلك.

4. **بطاقات الوفاء (delted card):** تعرف بطاقة الوفاء بأنها عقد يتعهد بمقتضاها مصدر البطاقة بفتح إعتماد بمبلغ معين لمصلحة حامل البطاقة الذي يستطيع بواسطتها الوفاء بمشترياته لدى المحلات التجارية التي ترتبط مع مصدر البطاقة بعقد يتعهد فيه بقبول الوفاء بثمن مشتريات، على أن تتم التسوية النهائية حسب المدة المحددة في العقد.

وقد تطورت وسيلة الدفع باستخدام هذه البطاقات، حيث أصبح الدفع يتم إلكترونيا وبأن يمنح حامل البطاقة رقما سريا (توقيع إلكتروني) يستخدمه في عملية الدفع والتحويل الأموال عبر شبكة الانترنت أو شبكة خاصة.

وهناك بطاقات عديدة يتم عمل بها في دول الكبرى الذي لها إقتصاد كبير يتطلب تسهيلات وسرعة في المعاملات التجارية والتي يتطلب بطاقات تتماشي مع هذا التطور منها بطاقات الصرف البنكي، البطاقات الذكية، بطاقات الموتدكس ...إلخ.[67]

إن عملية الدفع الإلكتروني كما ذكرنا سابقا متعددة الأطراف عبر الأنترنت مما يؤدي إلى ضعاف النفوس بالدخول إلى سوق بطاقات الأئتمانية من أجل إساءة إستعمالها في التزوير والنصب على التجارة والبنوك وتعدد صور الإعتداء في هذا المجال ولعل أبرز الصور في الوقت الراهن:

---

[67] - نضال إسماعيل ابراهم، المرجع السابق،ص: 87 ومابعدها.

– إساءة إستعمال البطاقات الدفع الإلكتروني من حامل البطاقة: ويقصد بحامل البطاقة هو الشخص الذي حصل عليها عن طريق البنك بمقتضى إتفاق بينهما ومنه يتحدد إلتزامات كل طرف، وأساليب التلاعب حامل البطاقة أو العميل كثير نذكر منها:

– الحصول على بطاقة إئتمان صحيحة بناء على مستندات مزورة مثلا:

أن يتقدم شخص إلى بنك وهو ينتحل صفة الغير وأن يقدم بيانات مزورة ومنه، لا يتمكن البنك إسترداد قيمتها لعدم إستدلال على صاحب البطاقة لعدم تقديم البيانات الكافية.

– الغش الذي يرتكبه الحامل البطاقة ويحدث الغش هنا في فرضيتين:

الحالة الأولى: أن يتم العقد بين العميل والبنك، فيجب على العميل رد البطاقة عند إنتهاء صلاحيتها إلى بنك، ولكن قد يقدم العميل إلى إستخدامها رغم إنتهاء مدتها، وقد نصت محكمة فرنسا بأن ذلك الفعل يعد خيانة أمانة لأن العميل إستعمل البطاقة من أجل وظيفة محددة، وأن إستمرار في إستعمال البطاقة يعد إختلاسا يضر بالبنك.

ويرى جانب من الفقه الفرنسي بأن التسليم البطاقة الإئتمانية للعميل يعد من عقود الأمانة ومنه. إساءة في إستعمالها يعد جريمة خيانة الأمانة وليس في مقام جريمة النصب لأن العميل قام بالكذب مجرد ولم يكن بطرق إحتيالية.

الحالة الثانية: إستخدام البطاقة بعد إلغائها من قبل البنك، ومنه يعد سلوك من قبيل الطرق الإحتيالية، ولذلك يتعين القول بأن العميل أساء إستخدام بطاقة الائتمان أو إرتكب غشا معلوماتيا، ومنه تعد جريمة ويكون تجريمها وفقا للنصوص خاصة يعاقب عليها في قانون العقوبات.[68]

– إساءة استعمال البطاقة البلاستيكية من قبل الغير: وهو في حالة السرقة أو الضياع البطاقة أو الرقم السري خاص بها، فيقوم الغير بتزوير البطاقة أو استبدال بياناتها أو السحب عن طريق بطاقات ائتمانية مسروقة.[69]

[68] - عبد الفتاح بيومي حجازي، المرجع السابق، ص: 121-122

[69] - محمد حسين منصور، المرجع السابق، ص: 123.

وفي هذه الحالة يجب على العميل في حالة ضياع أو السرقة أن يبلغ البنك المصدر لها حتى لا يتحمل مسؤولية المبالغ التي تسحب من رصيده ، فإن تقاعس عن تبليغ بفقد الرقم السري و اكتفى بإبلاغ عن فقد البطاقة فهو ملزم بالمبلغ التي سحبت من الغير و يرى جانب من الفقه الجنائي حيث يعتبرها جريمة نصب لأن الشخص انتحل صفة الشخص الحقيقي ببيانات كاذبة، وقد قام بإستعمال البطاقة بطرق إحتيالية ويرى البعض أنها جريمة سرقة لإستعمال المفاتيح المصطنعة.

وقد يحدث تواطؤ مابين الحامل الشرعي للبطاقة والغير بحيث يسمح الأول بإستعمال البطاقة في السحب وتزوير والتوقيع غير أن الحامل الشرعي يعترض عن عمليات السحب بطعن بالتزوير حتى لا يقع السحب من رصيده.

– تلاعب موظفي البنك المصدر البطاقة: ويكون لاتفاق ما بين الموظف والعميل حامل البطاقة أو مع التاجر أو مع الغير، بحيث يقوم الموظف البنك بإستخدام بطاقات سليمة بيانات مزورة، السماح للعميل بتجاوز حد السحب، أو سماح العميل بسحب ببطاقة منتهية الصلاحية أو بعد صدور توقيفها.

وقد يتلاعب موظف البنك مع أفراد العصابات الإجرامية ويسمح لهم بسحب المبالغ بطاقات صحيحة ومتداولة بدون وجه حق.

– التلاعب في بطاقات الوفاء من قبل التاجر: كقيام بعض التجار بإستخدام بطاقات ليست لها أرصدة كافية للصرفها من بنك ثم يتضح عدم وجود أرصدة لأصحاب هذه البطاقات والتلاعب في البرامج الخاصة في الماكينة الإلكترونية بحيث يعطل العمل بها أثناء قراءة البطاقة حتى لا يمكن من إكتشاف أنها مزورة.

– التلاعب في بطاقات الائتمان عن طريق شبكة الأنترنت:

وهناك عدة طرق يتبعها قراصنة الحاسب الآلي والأنترنت في الحصول على بيانات بطاقات الدفع الإلكتروني وإستعمالها بطرق غير مشروعة للحصول على السلع والخدمات وهذه الطرق:

– الإختراق الغير المشروع لمنظومة خطوط الإتصالات العالمية وهو ما يعرف باسم (Illegal Access) وهي خطوط تربط الحاسب الآلي للمشتري والمشتري، ويعد الجاني

الشخص الذي يتنصت على المكالمة الهاتفية، ويعد أسلوب خطير في التجار عبر الشبكة والدوافع إلى ذلك العمل الإجرامي.

وهو الرغبة الكامنة في قهر النظام التقنية والتفوق على الحماية المقررة لها، ودافع الرئيسي لهذه العصابات هو الحصول على أرقام الخاصة بالبطاقات المملوكة للغير وذلك عبر الشبكة الأنترنت، رغم صعوبات في عدم تحديد شخصية هؤلاء المجرمين.

ويمكن تحديد زمان الاختراق، وكيفية ذلك بمراجعة الملفات الدخول للنظام مما يسمح لمعرفة أكبر قدر من الآدلة التي تشير إلى الجاني.

تقنية التفجير الموقع المستهدف: وهذا الأسلوب يهدف بإرسال عدد كبير من الرسائل الإلكترونية من جهاز الحاسب الآلي إلى جهاز المستهدف بحيث تشكل هذه الكمية الكبيرة من الرسائل الإلكترونية ضغطا يؤدي بطبيعة الحال إلى تفجير الموقع، ويسهل على المجرم التنقل بحرية ويسر وحصوله على كل الأرقام والبيانات التي تفيده.

– أسلوب الخداع: ويتحقق هذا الأسلوب بخلق مواقع وهمية على شبكة الانترنت لاستقبال المعاملات المالية الخاصة بالموقع الحقيقي أي الأصلي، ولهذا يتوجب إتخاذ إجراءات أمنية لمنع الإساءة إستخدام البطاقات الدفع الإلكتروني، وزيادة رسائل الحماية التقنية أكثر من إنتاج التقنية نفسها.[70]

المطلب الثالث: تنفيذ الالتزام الالكتروني

العقد الصحيح يترتب عن تنفيذ الالتزامات الناشئة عنه. إلا أنه في بعض الأحيان لا يتم تنفيذ العقد و ذلك لعدة فروض منها :

– **الإخلال بالالتزام الإلكتروني:** العقد الذي تضمن كل الشروط اللازمة له أصبح واجب التنفيذ ويقتضي كل طرف في العلاقة لتنفيذ ما يقع على عاتقه من التزامات، فإذا لم يقم المدين بتنفيذ الاختياري كان من الممكن إجباره على التنفيذ وهو التنفيذ العيني الجبري،

[70]- عبد الفتاح بيومي حجازي، المرجع السابق ص 124 وما بعدها.

ويحق للدائن المطالبة بالتعويض في حالة عدم التنفيذ. وهذا مترتب عن المسؤولية العقدية.

ويتضح أن الخطأ العقدي وهو عدم تنفيذ المتعاقد لالتزامه الناشئ عن العقد بحيث أن الخطأ يتوفر إذا لم يقم المدين بتنفيذ التزامه كله أو بعضه أو قام بالتنفيذ على نحو يخالف الوجه المتفق عليه أو الذي يوجبه القانون. مثلا كتسليم بضاعة فيها عيب أو ناقصة الجودة المتفق عليها أو تأخير في تنفيذ عن الموعد المحدد لذلك.

ويثور المشكل هنا في حالة التنفيذ المعيب، حيث أن في مجمل العقود يتسم غالبها بطابع البعد سواء في تمثيل المنتج أو الخدمة ويستلزم أن يغلب عليها من حسن نيته في التنفيذ، خاصة في مواجهة المستهلك غير المحترف، والأمثلة على ذلك كثيرة، تقديم للعميل ببرامج حاسب الآلي أو أجهزة لا تتفق واحتياجاته، أو سوء الخدمة بالنسبة لعقود الاشتراك في شبكة الإنترنت والفضائيات والمحمول.[71]

– **طبيعة الالتزام الإلكتروني:** إن عدم تنفيذ تختلف صوته بحسب الالتزام فهناك نوعان من التزام:

التزام بتحقيق غاية أو نتيجة، والتزام ببذل عناية أو بوسيلة، نجد أن طبيعة المعاملات الإلكترونية في أغلبها يتسم بتحقيق نتيجة حيث يبذل المدين جهوده للحصول على النتيجة المرغوب فيها من محل التزام، وعلى المدين أن يثبت أنه قام بالتنفيذ أي تحقيق النتيجة المرجوة، فإذ لم ينجح في ذلك قامت مسؤولية العقدية، ولا يستطيع أن يتهرب من المسؤولية إلا أن يثبت العكس وأنه قد بذل كل ما في وسعه ويرجع أن عدم التنفيذ راجع إلى عنصر أجنبي لا دخل له فيه "كقوة قاهرة أو لخطأ الدائن".

وفي معظم المعاملات الإلكترونية الأخرى يتسم بعضها إما بتسليم بضاعة أو تقديم خدمة وتبدو المشكلة في حالة ما إذا كان المدين يقدم سلعة بحالتها وردت له من المنتج، ويتذرع بأن كل ما عليه هو بذل العناية في التحقيق منها وعرضها بصفاتها كما هي.

---

[71] - محمد حسين منصور، المرجع السابق ص 84 و 85

وفي حالة ما إذا كان محل الالتزام هو تقديم خدمة، فهناك خدمات يلتزم مقدمها بتقديم أحسن خدمة للعملاء، كخدمات القنوات الفضائية أو التلفون وشبكة الإنترنت ... إلخ، ويبذل عناية في توصيل الخدمة، غير أنه هناك شركات تستقبل مشتركين كثيرين، مما يزداد الضغط عليها فلا يستطيع أن تقدم أفضل خدماتها وهنا ينقل التزام.

ويمكن تحديد ما إذا كان موضوع الالتزام بالنظر إلى ما اتجهت إليه إرادة المتعاقدين. وبالنظر إلى النتيجة المنتظرة من وراءه إما أن تكون مؤكدة أو احتمالية. وبالنظر إلى ظروف التي نشأ فيها التزام يمكن أن تكشف عن طبيعة فإذا كانت الظروف العادية أي العناية المعتادة فهذا يؤدي إلى نتيجة مؤكدة. أما إذا كانت اليقظة لا تؤدي بالضرورة إلى النتيجة المرجوة الذي يهدف المدين إلى تحقيقها وهنا كنا بصدد التزام بذل عناية.

وفي حالة ما إذا طبقنا القواعد السابقة على عقود الخدمات الإلكترونية فالنتيجة المرغوب فيها من وراء التزام هو تحقيق نتيجة وهو ما تتجه إليه إرادة الطرفين. أما ببذل عناية فيكون بتطوير التقنيات لتقديم أفضل خدمة مما يجعل النتيجة مؤكدة، أما إذا كان هناك إهمال وتقاعس من جهة الشركات لتوفير أحسن الخدمات وتعميق معداتها رغم حرصها على قبول عدد كبير من المشتركين، فهنا يقوم التزامها لتحقيق نتيجة حتى لو تحفظت غير أنه لا يعرفها من المسؤولية لأنه يتسم بالتعسف في مواجهة المستهلك في هذا العقد الذي يتسم بصفة الإذعان. 72

الفرع الأول: المسؤولية العقدية عن فعل الشيء والغير وتعديل قواعدها

هناك بعض الحالات يرجع إلى عدم تنفيذ لمحل التزام إلى تدخل إيجابي من دراسة الشيء الموجود في حراسة المدين، فتثور المسؤولية العقدية عن فعل الشيء ونجد مثال في المعاملات إلالكترونية بسبب التقدم التكنولوجي أو الخطأ في تشغيل البرنامج على نحو يتسبب في الأضرار بالأجهزة التي تعتمد عليه وسلامة الأشخاص، أو تزويد بمعلومات خاطئة للعميل مما يتسبب عن ذلك من أضرار له أو للغير، وقد يستعين المتعاقد أحيانا بغيره لمساعدته في التزامه العقدي فقد يتسبب أحد المساعدين

[72]- محمد حسين منصور، مرجع السابق، ص 86 وما بعدها.

بخطأ مما يؤدي إلى عدم تنفيذ العقد فهنا يثور المسؤولية عن فعل الغير. وتقوم هذه الأخيرة بسبب الإخلال وذلك بغض النظر ما إذا كان الشخص يعمل لديه بصفة دائمة أو عرضية، بمقابل أو بغير مقابل، وتتوضح تلك المبادئ في المعاملات إلالكترونية بحيث تتولى الشركات المتعاقدة بتنفيذ التزاماتها من خلال العاملين لديها وممثليها ومندوبيه ا والمقاولين من الباطن، لذلك تثور مسؤولية الشركات عن الأفعال الضارة التي تصدر من أشخاص السالفة الذكر.

وقد تعمد بعض الشركات المتعاقدة إلى تنظيم أحكامها وتضمين العقد شروطا للإعفاء أو التخفيف من المسؤولية فتقوم بتحويل التزامها بتحقيق نتيجة إلى التزام بذل عناية فلا تتحقق مسؤوليتها إلا إذا أثبت الدائن تقصيرا منها في بذل العناية المطلوبة مثلا كالنص في عقود الخدمات الأنترنت والمحمول والفضائيات على إلتزام بتقديم أحسن خدمات ممكنة، تنص على عدم المسؤولية عن الأضرار الناجمة عن سوء الإستعمال أو عدم إلتزام بالتعليمات، أو المخاطر البيئية المحيطة مثل الظروف الجوية أو إنقطاع التيار الكهربائي، وأيضا فمن عدم تحمل مخاطر التي تحدث للسلعة أو المنتج أثناء الشحن أو في الطريق حيث تسمح للمتعاقد بالتهرب من المسؤولية في مواجهة المستهلك الذي يجدر حمايته من تلك الشروط التي تتسم بالتعسف بسبب العقد الذي يتصف بأنه عقد إذعان.73

الفرع الثاني: وقف العقد وانحلاله (جزاء عدم تنفيذ)

يمكن أن تطرأ بعض العقبات التي تحد دون تنفيذ العقد بصفة مؤقتة أي وقفة بناء على إتفاق الأطراف أو طرأت قوة قاهرة مؤقتة تمنع الإستمرار في التنفيذ مثلا كحظر الدول الإستيراد لمدة معينة، أو منح القاضي أجلا للمدين مدة لتنفيذ إلتزامه.

والوقف كجزء هو الأسلوب الجاري إتباعه في المعاملات الإلكترونية حيث يحمل وجهين: الأول الإخلال بالالتزام والثاني وسيلة فعالة للضغط على التعاقد لتنفيد إلتزامه، وفي معظم الشركات تأخذ بهذا الأسلوب في حالة ما إذا أخل العميل بالتزامه بدلا من اللجوء إلى التنفيذ العيني الجبري أو النسخ بدلا من اللجوء إلى القضاء الذي

[73] - محمد حسين منصور، المرجع السابق، ص 89. 90

يؤدي بالضرورة إلى خسارة العميل أو تقوم جهة الموردة بالخدمة بوقفها كما هو الحال بالنسبة لخدمة الهاتف المحمول أو الأنترنت.74

ولذلك إذا تعاقد مشتري مع بائع على سلعة ما، ولم يقم البائع بتسليم السلعة في محل المتعاقد فإن لم يكن المشتري قد دفع الثمن، فيمكن له أن يدفع بعدم التنفيد للإلتزام المتوجب عليه.

والأساس الذي يقوم عليه الدفع بعدم التنفيد هو مايسمى نظرية السبب المباشر بمعنى أن بسبب إلتزام المتعاقد هو إلتزام المتعاقد الآخر.75

ويجوز للمتعاقد التمسك بالدفع في مواجهة المتعاقد الآخر الذي يطالبه بالتنفيذ دون الحاجة إلى القضاء ويترتب عن ذلك توقف التنفيذ طوال المدة التي لا يتم فيها تنفيذ الإلتزام بالمقابل: فالدفع لا يؤثر على وجود العقد ولا يؤدي إلى زوال الإلتزام بل يبقى كما هو دون نقص في مقداره.76

ومن المهم التنبؤ إلى عدم إمكانية استمرار الامتناع عن التنفيذ وإنما هو إجراء مؤقت إذا لم يعط آثاره فللقاضي أن يقرر الفسخ أو التنفيذ العيني الجبري، أو أن ينتفي الدفع بتقديم المدين ضمانا يكفل أن ينفذ إلتزام التسليم.77

والمتعاقد الذي يتمسك بالدفع لا يعد مقصرا في عدم الوفاء ولا تقوم عليه أية مسؤولية ولا يكون مسؤولا عما يلحق الطرف الآخر من ضرر من جزاء عدم تنفيذه الإلتزام الذي يدفع بعدم تنفيذه.

ويجوز للمتعاقدين للتحلل من العقد بحيث يجوز للقانون في بعض الحالات إنهاء العقد إما بالإدارة المتعددة كما يمكن أن يتفق الطرفان على نقض العقد، كما يلجأ في بعض الأحيان المتعاقدين إلى الفسخ للتحرر من رابطة عقدية الفاشلة، في حالة إخلال

---

[74] – محمد حسين منصور، المرجع السابق ص: 90 و 91.

[75] – نضال إسماعيل برهم، المرجع السابق، ص: 81.

[76] –محمد حسين منصور، نفس المرجع، ص 91

[77] – نضال اسماعيل برهم، مرجع السابق، ص: 81

الطرف الآخر بإلتزامه، ويتم ذلك باللجوء إلى القضاء كما يجوز أن يتضمن للعقد على الشرط صريح بالفسخ، أي أعتبر العقد مفسوخا من تلقاء نفسه دون اللجوء إلى اعدار اوصدور حكم قضائي بمجرد اخلال المدين بالتزامه . ولا ينتهج في المعاملات الإلكترونية الطريق التقليدي في إنهاء العقد لما تسبب به هذا الأخير من مشاكل وعراقيل، الذي يجري العمل على تمسك كما سبق، يوقف العقد أو الدفع بعدم التنفيذ وفي حالة الضرر يلجأ إلى إنهاء العقد.78

78 – محمد حسين منصور، مرجع السابق ص 94

الفصل الثاني

الاعتداء على نظام عمل التجارة الالكترونية

خاتمـــــة:

آلية قيام و نماء التجارة الالكترونية هو الانترنيت أو شبكة الانترنيت و تعمل هذه التجارة على كسب ثقة المتعاملين بها و لكون أن النشاط التجاري يقوم على ركني السرعة و الائتمان فإن الركن الأول و إن تحقق بفضل تكنولوجيا الاتصالات، فإن الركن الثاني الذي هو الائتمان ينبغي أن يصرف فيه المشرع جهده لتوفير عامل الثقة لدى المستهلك حتى تنمو هذه التجارة، فليس يخفى على أحد ما لخطورة إيداع تفاصيل بطاقة ائتمانية أو وضع بيانات شخصية أو أرقام حسابات على شبكة مفتوحة مثل الانترنيت، و لكون أن مواقع التجارة الالكترونية ترتكز على نظام معلوماتي مستند كغيره من الأنظمة إلى قاعدة بيانات فإن أي خطر يتهدد النظم المعلوماتية، يهدد هو أيضا – بأن صورة يحدث بها هذا التهديد – هذه التجارة أي يستهدف مواقعها ويضر بخصائص السرعة ،الائتمان و السريّة.

تمهيد :

جرائم التجارة الالكترونية كغيرها من الجرائم المستحدثة هي حصيلة اتساع حجم التعامل الإنساني مع ظاهرة المعلوماتية في تلك الفترة الوجيزة حيث نتج عن ذلك التفعيل مصطلحات التفاعل الايجابي مع التقنية ففرز بدوره تفاعلا إنسانيا سلبيا بدا في السلوكيات الاجتماعية المنحرفة نشوءا وتطورا من ناحية الأساليب و الآثار هذه النواحي السلبية هي ما يتجلى في الجرائم المعلوماتية. وجرائم التجارة الالكترونية هي احد أنماط هذه الجرائم والتي ينضر لها من ناحية ضبطها بتعريف إلى تصنيفها كما يلي:[79]

- تعريفات باعتبار وسيلة ارتكاب الجريمة
- تعريفات باعتبار موضوع السلوك الجريمي.
- تعريفات باعتبار توافر المعرفة بتقنية المعلومات.
- تعريفات باعتبارات أخرى مختلفة.

ولعل الذي ينطبقه بن تعريفات في ذلك على جرائم التجارة الالكترونية هو لاعتبار الثاني أي موضوع الجريمة و في ذات الاعتبار تعددت التعريفات أيضا لكن يمكن إجمالا حصر نقاط اتفاقه بين تلك التعاريف فيما تعلو موضوع التجارة الالكترونية بان يراعي في هذا الاعتبار أولا جانبان

1 - أن يتلاءم التعريف مع آلية التعامل التجاري أي أن يكون منطقيا تماما على المعاملات التجارية الالكترونية من جهة ومن جهة ثانية ان يكون متفقا مع فكرة عالمية التعامل أي ان يكون التعريف مقبولا و مفهوما على مستوى دولي و عالي.

2 - أن يسمح التعريف باستيعاب ما قد يستحدث من صور أخرى للجريمة في نطاق معاملات التجارة الالكترونية بفعل التطور المستمر لتقنية المعلوماتية و شبكة الانترنيت، و أن لا يقتصر فقط على التكنولوجيا الحالية.

[79]- محمود رشيد، قضايا، ص 21.

وثانيا نجد أن نقاط الاتفاق بين هذه التعاريف هو ما نستخلصه فيها ما يلي:[80]

- كل أشكال السلوك غير المشروع الذي يرتكب باستخدام الحاسب الآلي من التي بيناها سابقا.
- كل شكل تؤدي فيه البيانات و برامج المعلومات دورا رئيسيا.
- أية جريمة يتطلب لدى فاعلها معرفة تقنية الحاسب و المعلوماتية.
- كل فعل أو امتناع من شأنه أن يشكل اعتداء على مراكز قانونية بطريقة مباشرة أو غير مباشرة ناتج عن تدخل التقنية المعلوماتية.

و لعل الباعث على الاختلاف في تعريف هذا النمط من الجرائم كونها جرائم حديثة ذات مفاهيم و أبعاد متعددة بتنوع صورها و أنماطها و تطورها (أي تحديد أو استحداث صور جديدة).

المبحث الاول: (مواقع التجارة الإلكترونية)

إن الحكومات كما الأفراد على وعي تام بضرورة و حتمية الانخراط في المنظومة المعلوماتية لما توفره من مزايا أمام تعقيدات الحياة المتطورة و مدى إسهامها في تحديث البنى التحتية الدافعة للتنمية الاجتماعية المتكاملة و مدى توفيرها لمزيد من الخيارات أمام المتعاملين بها بفعل عامل المنافسة، فقد أفرز تفاعل النشاط البشري مع عامل ثورة الاتصالات علاقة كونت ظاهرة إنسانية حققت ظواهر اجتماعية غير مسبوقة في خرقها لعامل الزمن و إزالتها لكل الحدود الزمنية و المكانية

أدى حجم التعامل الإنساني مع ظاهرة المعلوماتية في فترة حديثة و وجيزة إلى استحداث مصطلحات التعامل الإيجابي مع التقنية الرقمية كما هو الشأن في التجارة الالكترونية، حركة البريد الالكتروني، التداول الأكاديمي وغيرها من المجالات على أن هذا الجانب الإيجابي خلق نقيضا في الجانب الآخر، حيث أضحى هناك تفاعل إنساني سلبي ظهر في نمط جديد من الجريمة، له تبعات عكسية أكثر خطورة من الظاهرة

[80]- محمودرشيد، قضايا، ص 22.

الإجرامية التقليدية، تجلى في ما بات يعرف بالجريمة المعلوماتية أو الالكترونية. ولما لم يكن هناك فرق بين النظام التجاري التقليدي وما استحدث من تقنية التعاملات التجارية الحديثة عدا آلية التعامل [81] ، فبقدر ما حمى المشرع المراكز القانونية الناشئة عن التجارة التقليدية بقدر ما هناك مصالح ينبغي أن تحمى و حقوقا ينبغي أن تسنّ لها النصوص الكافلة لها تلك الحماية.فإذا كان من المعلوم أن الجريمة قرينة التطور العلمي، فإنه من البديهي أن يتوازي ظهور أنماط الجريمة مع التطور التكنولوجي تتعلق بسرية المعلومات، الاعتداء على الخصوصيات الثقافية و الاجتماعية، حماية المستهلك، تداول البيانات الخاصة و غيرها من الجرائم التي تضر بالحقوق المقررة الأشخاص و المحمية قانونا أصلا، فهل أعدت التشريعات الدولية والإقليمية والوطنية إستراتيجية تتصدى للأفراد و الجماعات الذين احترفوا الإجرام المعلوماتي وتخطوا به كل الحدود المشفرة[82].

والتجارة الإلكترونية بارتكازها على شبكة الإنترنيت – التي هي نظام معلوماتي يتم بواسطة المبادلة التجارية– هو حاجة عاجلة إلى كفالة حماية جنائية لنظام ومواقع التجارة الإلكترونية لأجل حماية مضمون النشاط ذاته ولن يتأتى ذلك إلا من خلال منظومة تشريعية ترتكز على تجريم ما يلي83:

المطلب الاول: الدخول غير المشروع لمواقع التجارة الإلكترونية

يشكل هذا الفعل أحد الاعتداءات الماسة بالأنظمة المعلوماتية والتي تشكل بيانات التجارة الإلكترونية أحد أنظمتها لذا وجب التطرق لها بالدراسة

ولعل المشرع الجزائري في إطار عصرنة منظومته تشريعية استدرك القصور الوارد في النص على مثل هذه الجرائم وكفالة حماية للمصلحة المحميّة في تعاملات التجارة الإلكترونية وذلك من خلال تعديله لقانون العقوبات وبالضبط ما أورده في الفصل الثالث

---

[81] **Agathe LEPAGE, Libertés sur l'Internet et cybercriminalité : les apports au droit pénal de la loi pour la confiance dans l'économie numérique du 21 juin 2004, Revue Droit pénal n° 12, Décembre 2004, Etude 18**

[82] **Agathe LEPAGE, Libertés sur l'Internet et cybercriminalité : les apports au droit pénal de la loi pour la confiance dans l'économie numérique du 21 juin 2004, Revue Droit pénal n° 12, Décembre 2004, Etude 18**

[83] عبد الفتاح بيومي حجازي: النظام القانوني لحماية التجارة الإلكترونية، دار الفكر الجامعي، الإسكندرية2004،ص 9-11

من الباب الثاني من الكتاب الثالث من الأمر 156/66 في القسم السابع مكرر عنوانه المساس بأنظمة المعالجة الآلية للمعطيات ويشمل المواد 394 مكرر إلى 394 مكرر84

والجرائم التي يتصور المشرع الجزائري وقوعها على نظام المعالجة الآلية للبيانات والمعطيات والتي تنسحب بالطبع على مواقع التجارة الإلكترونية تشمل الصور التالية :

الدخول أو البقاء غير المشروعين ، نظام المعالجة الآلية للمعطيات.

الاعتداءات العمدية بإعاقة أو تحريق تشغيل نظم معالجة بيانات التجارة الإلكترونية.

الاعتداء العمدي على سلالة المعطيات الموجودة داخل النظام.

وقد أفرد لها عقوبات أصلية وأخرى تكميلية لتلك الجرائم وهذه الجرائم أي جريمة الدخول أو البقاء غير المشروع في نظام المعالجة الآلية للمعطيات أو في جزء منه، مع النص على ظرف مشدد لتلك الجريمة إذا نتج عن الدخول أو البقاء محو أو تعديل معطيات النظام أو إفساد وظيفة النظام وجريمة عرقلة أو إفساد النظام لأدائه لوظيفة وجريمة إدخال غير مشروع لمعطيات في نظام المعالجة بآلية المعطيات أو المحو أو التعديل غير المشروع للمعطيات التي يحتويها (وإن اختلفت في أركانها) وما يقابلها من عقوبات أصلية وتكميلية وكذا مسؤولية الشخص المعنوي ومعاقبة الشروع في مثل هذه الجرائم وكذلك الأعمال التحضيرية الجماعية (الاتفاق الجنائي) و دراسة هذه الجرائم تقتضي بيان مفهوم نظام المعالجة الآلية للمعطيات كون أن الحكم على الشيء فرع عن تصوره.

الفرع الأول : مفهوم الدخول إلى النظام والبقاء غير المشروع فيه :

تقع هذه الجريمة من طرف أي شخص كانت صفته ويكون من بين أولئك الذين لهم حق الدخول إلى النظام ، وهذه الجريمة تقع متى كان الدخول مخالفا صاحب النظام أو من له حق السيطرة عليه كالأنظمة المتعلقة بأمن الدولة أو أنظمة يتعلق مجموعة الحياة الخاصة التي لا يجوز الإطلاع عليها أو أن يكون الجاني قد خرق قيد الدخول الموضوع أن أو أن يتطلب الجاني لم يسدد مبلغا مستحقا للدخول ينبغي سداده وقام بالدخول، والمشرع الفرنسي عاقب على مجرد الدخول دون تحديد وسيلة الدخول إلى النظام سواء عن طريق كلمة السر أو برنامج تشفير خاص أو استغلال شخص تخول له

84أما المشرع الفرنسي فقد نص عليها في الباب الثالث من القسم الثاني من الكتاب الثاني من قانون العقوبات الفرنسي الجديد وورد النص عليها في المواد 1/323 إلى 7/323،أنظر آمال قارة ،مرجع سابق ، ص، الحماية الجزائية المعلوماتية في التشريع الجزائري ، دار هومه ، الجزائر، 2006.ص 100.

بالدخول، ومجرد الدخول إلى النظام المعلوماتي تقوم به الجريمة به حتى ولو لم يترتب على دخوله ضرر أو لم يحقق فائدة من الدخول سواء كان الدخول تم إلى النظام كله أو إلى جزء منه ويجرم كل شخص بالدخول غير المشروع متى كان مسموحا للجاني بالدخول إلى جزء معين من برنامج وتجاوزه إلى جزء آخر غير مسموح له بالدخول فيه [85].

والهدف من تجريم فعل البقاء غير المشروع داخل نظم المعالجة الآلية للمعطيات هو قيام مسؤولية الجاني عن جريمة عمدية لأن إرادته انصرفت إلى البقاء داخل النظام مع علمه بأن دخوله غير مأذون له به والحكم منصرف إلى من هو مسموح له بالدخول إلى جزء من النظام ثم يدخل إلى جزء غير مصرح له بالدخول فيه [86] ، ويرى جانب من الفقه أن هذه الجريمة يقوم بسلوك سلبي فالجاني وإن كان دخوله إلى النظام تم بطريق الصدفة وانتفى لديه القصد الجنائي ، لكن رقم علمه بأن هذا الفعل غير مشروع فإن إرادته تنصرف إلى البقاء داخل النظام ، ويرفض الخروج منه ويمتنع [87].

ويتخذ فعل البقاء داخل النظام صورة الجريمة المستمرة ذلك أن وفقا للرأي الذي سلف فإن فعل البقاء من صورة البقاء المعاقب عليه أن يضل الجاني بأعياد داخل النظام بعد المدة المحددة له البقاء داخله أو في حالة أن ينسخ معلومات معروضة فقط للإطلاع أو أن يحصل الجاني على خدمة أن يدفع مقابلا المقررة لها[88].

وقد تضبط هذه الفكرة أيضا أي فكرة الدخول غير المشروع بكونها "التسلسل داخل النظام المعلوماتي أما الدخول من حيث الزمان فيتمثل في تجاوز حدود التصريح أو الترخيص داخل النظام والممنوح لفترة زمنية محددة تجاوز هذه الفترة الزمنية" [89]، كما يلحق بها ما يدخل في نطاق الغش المعلوماتي الذي لا يقع الاعتداء فيه على

---

[85] علي عبد القادر قهوجي ، الحماية الجنائية لبرامج الكمبيوتر،المكتبة القانونية، القاهرة، 1999، ص132،131

[86] **Hubert BITAN , Le site de commerce électronique : approche technique et juridique, Revue Gazette du Palais, 18 avril 2000 n° 109, P. 17**

[87] احمد حسام طه أحمد حسام طه تمام ، مرجع سابق ، ص الجرائم الناشئة عن الحاسب الآلي أطروحة دكتوراه ،جامعة القاهرة 2000،ص ، 299، ويعرف هذا الفعل بأنه التواجد داخل نظام المعالجة الآلية للمعطيات ضد إرادة من له الحق في السيطرة على هذا النظام ،للاطلاع انظر:

-La protection juridique des bases des donnees electroniques, petites affiches LPA, france 28 avril 1995, n° 51 ,p.14

[88] علي عبد القادر قهوجي ،مرجع سابق، ص52

[89] عبد الفتاح بيومي حجازي ، مرجع سابق،ص 32

الوظائف الطبيعية للحاسب الآلي أو تعديل بيانات المعالجة بل يقع الدخول إلى مركز معالجة البيانات في الحاسب الآلي بأداة الكترونية وظيفتها أو تعمل على التقاط المعلومة أو التنصت مثلا.[90]

الفرع الثاني : جريمة الدخول و البقاء غير المشروعين في صورتها البسيطة:

تتحقق الجريمة بصورتها البسيطة بفعل الدخول غير المشروع متى توافر القصد بعنصريه العلم و الإرادة عند الجاني الذي اخترق النظام أو بقي فيه، ذلك أن جريمة الدخول إلى النظام أو البقاء فيه هي من الجرائم العمدية التي تقوم بالقصد الجنائي العام، فيفترض لقيامها بصورتها البسيطة علم الجاني بأنه لا يحق له الدخول أو البقاء داخل النظام، و أن هذا الفعل تم ضدّ إرادة صاحب النظام أو مالك السيطرة عليه، فإرادة الجاني منصرفة إلى إتيان الفعل بانتهاك صاحب الحق و بمخالفة القانون [91] و بذلك يقوم الركن المادي للجريمة في صورته البسيطة، و قد عاقب المشرع الفرنسي عن هذه الجريمة بهذه الصورة بالحبس لمدة سنة و غرامة 100.000فرنك فرنسي، و ضاعف هذه العقوبة في الصورة الثانية للجريمة.

الفرع الثالث : جريمة الدخول إلى النظام أو البقاء غير المشروعتين في صورتها المشددة :

نص المشرع الجزائري على عقوبة هذه الصورة المشددة في المادة 394 مكرر 3/2 بقوله: " تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة و إذا ترتب عن الأفعال المذكورة أعلاه تخريب لنظام اشتغال المنظومة تكون العقوبة الحبس من ستة أشهر إلى سنتين و الغرامة من 50.000 إلى 150.000دينار جزائري، كما أن المشرع الفرنسي رفع درجة العقوبة على هذه الجريمة إذ كيّفت بصورتها المشددة، إلى الحبس سنتين و غرامة 200.000 فرنك فرنسي.

و تتحقق الجريمة في صورتها المشددة إذا نتج عن الدخول أو البقاء غير المشروع محو أو تعديل البيانات التي يحتويها النظام أو تعطيل النظام ويتحقق الظرف المشدد بوجود علاقة سببية بين الدخول أو البقاء غير المشروع و نتيجة تلك النتيجة الضارة أي عدم صلاحية النظام للقيام بوظائفه و عدم قدرته على أداء وظيفة المعالجة الآلية للبيانات أو المعلومات.

---

[90]- احمد حسام طه أحمد حسام طه تمام ، مرجع سابق ، ص،مرجع سابق،ص 300.

[91]- علي عبد القادر القهوجي ، مرجع سابق ، ص مرجع سابق،ص 53.

و هذه الجريمة هي من الجرائم العمدية التي لا تقوم إلا بتوافر القصد الجنائي العام بعنصريه العلم و الإرادة، إلا أنه إذا أثبت الجاني انتفاء علاقة السببية بين السلوك الجرمي و الدخول أو البقاء غير المشروع في النظام و بين النتيجة الإجرامية (المحور أو التعديل أو تعطيل النظام) انتفى الوصف الإجرامي على السلوك و انتفى كذلك القصد الجنائي لدى الجاني كأن يثبت أن تعديل أو محو المعطيات أو أن عدم صلاحية النظام للقيام بوظائفه يرجع إلى القوة القاهرة أو الحادث المفاجئ[92].

و منه فإن تجريم الدخول أو البقاء غير المشروعين إلى النظام المعلوماتي هو ضمانة لنظم البيانات التي تحرك مواقع التجارة الالكترونية و تساهم في بعثها و حركيتها و بقدر تلك الثقة و السرية التي يرتكز عليها ركن الائتمان بقدر إقدام أو إحجام المتعاملين (منتجين كانوا أو مستهلكين) على التعامل بها لذا كان لزاما على المشرع – لأجل استثمار هذه التقنية– أن يتخذ كل ما هو ضروري من إجراءات و تدابير ضد من يمس أو يعتدي على سلامة نظم البيانات المتعلقة بمواقع هذه التجارة [93].

المطلب الثاني : الاعتداء العمدي على سير نظام المعالجة المتعلقة بالتجارة الالكترونية:

لم ينص المشرع الجزائري على هذا الجرم غير أن الاتفاقية الدولية للإجرام المعلوماتي نصت عليه في المادتين 05 و 08، أما المشرع الفرنسي فقد نص في المادة 2/323 من قانون العقوبات الجديد على عقوبة هذا السلوك الإجرامي و أفردها بعقوبة الحبس لمدة ثلاث سنوات و غرامة تصل إلى: 300.000 فرنك فرنسي في حق من قام بإعاقة أو إفساد تشغيل نظام معالجة البيانات[94].

و هذا السلوك المتوقع من شأنه إحداث اضطراب في نظام معالجة البيانات أو المعطيات و المعلومات المتعلقة بالبيانات المتواجدة على مواقع التجارة الالكترونية كيفما كانت أرقام حسابات، بيانات شخصية، بطاقات ائتمان... الخ ، كما أنه السلوك (الإعاقة أو الإفساد) الذي يستهدف إعاقة النظام لم يشترط المشرع له وسيلة معينة

---

[92] - خثير مسعود ، مرجع سابق ، ص ، الحماية الجنائية لبرامج الحاسب الالي، رسالة ماجيستير،جامعة تلمسان، الجزائر، ص ، 94.

[93] **Hubert BITAN , ...**

[94] - آمال قارة ،مرجع سابق ، ص، مرجع سابق ، ص 114.

لوقوعه و حصول الإعاقة، فبمثل ما قد يقع بوسيلة مادية قد يقع بآلية معنوية منطقية [95] بل ينصرف وصف السلوك الإجرامي في هذه الجريمة إلى كل نشاط من شأنه إرباك عمل النظام في إطار معالجة البيانات سواء أكان عمل الجاني منصرف إلى إعاقة نظام التشغيل و الإرسال أو منصرف إلى إفساده، و يستوي أيضا في السلوك الإجرامي أن يكون أثره ممتد إلى توقيف النشاط بصورة دائمة أو مؤقتة، و يستوي أيضا أن يكون الجاني قد أحدث فعله بوسيلة مادية أو معنوية ، فالوسيلة المستخدمة بالنسبة للمشرع واحدة، كما لا يشترط أن تكون الإعاقة أو الإفساد بصورة كلية بل يعتّد حتى بالإفساد الجزئي للنظام[96] كما لا يشترط أن يقع فعل التعطيل أو فعل الإفساد على كل عناصر النظام جملة، بل يعتمد بتأثر أحد هذه العناصر مادية كانت (الحاسب الآلي ذاته، شبكات الاتصال، أجهزة النقل) أو معنوية (البرامج و المعطيات)[97].

الفرع الاول : الركن المادي للجريمة

هذه الجريمة من الجرائم من العمدية ويتمثل الركن المادي لهذه الجريمة في فعل توقيف أو تعطيل نظام معالجة المعطيات عن أداء نشاطه الذي صمّم لأجله أو فعل إفساد نشاط أو وظيفة المعالجة الآلية لمعطيات كما سبق شرحه و صور هذا الاعتداء هي:

1- فعل التعطيل (التوقيف، العرقلة):

يفترض في هذا السلوك وجود فعل إيجابي، يندرج ضمن إعاقة النظام دون اشتراط وسيلة معينة لحصول الإعاقة فقد تكون تمت بطريقة مادية باستخدام العنف أو دونه على جهاز الحاسب الآلي أو شبكة الاتصال بتخريبها أو كسرها أو تحطيم الأسطوانة أو قطع شبكات الاتصال أو منع العاملين على الأنظمة من الوصول إلى المكان الذي توجد فيه الأنظمة، و تكون وسيلة الإعاقة أو التعطيل معنوية إذا وقعت على الكيانات المنطقية للنظام ليؤدي إلى أن يتباطأ النظام في آداء وظيفته و ذلك إما بالتلاعب في المدخلات أو التلاعب في البرامج و ذلك بإتباع إحدى التقنيات التالية:[98]

إدخال برنامج فيروسات

استخدام قنابل منطقية

---

[95] حجازي، مرجع سابق،ص 43

[96] - مدحت رمضان عبد الحليم ، مرجع سابق ، صعبد الحليم ،الحماية الجنائية للتجارة الالكترونية، دار النهضة العربية، ص 54.

[97] - علي عبد القادر القهوجي ، مرجع سابق ، ص مرجع سابق، ص 139.

[98] - آمال قار مرجع سابق، ص 115، 118.

استخدام بطاقات الوقف (وقف تنفيذ البرنامج)
إشباع إمكانيات الدخول (شغل النظام بمعطيات تفوق سعته)
جعل النظام يتباطئ في أدائه لوظائفه.

02-فعل الإفساد (التعييب):

يقصد بالإفساد ذلك الفعل الذي يجعل من نظام المعالجة الآلية للمعطيات غير قادر على الإشتغال بشكل سليم، بأن يعطي مثلا نتائج غير تلك التي يفترض الحصول عليها و الإفساد بهذا المعنى يقترب من التعييب الذي رأيناه في جريمة الدخول أو البقاء غير المشروعين في النظام إلا أن الفارق بينهم تحقق القصد الجنائي، حيث الإفساد في جريمة البقاء الدخول غير المشروعان بصورتهما المشددة لا يشترط فيهما أن يكون عمديا بينما مطلوب في هذه الجريمة أن يكون الإفساد متعمدا و لذلك سميت بجريمة الاعتداء العمدي أو القصدي على نظام المعالجة الآلية للمعطيات و على ذلك لا يكون الإفساد نتيجة إنما هو مضمون السلوك الإجرامي في هذه الجريمة، أما بخصوص تقنيات التعييب و الإفساد فهي متعددة منها[99]:

القنبلة المعلوماتية بحيث يدخل بواسطتها مجموعة من المعطيات تتكاثر داخل النظام و تجعله غير صالح للاستعمال

استخدام فيروس وظيفته القيام بتغيير غير محسوس في البرنامج أو المعطيات حيث تجعل مخرجات النظام غير تلك التي كان من المفترض أن يصورها.

الفرع الثاني :الركن المعنوي

جريمة الاعتداء العمدي (القصدي) على نظام المعالجة الآلية للمعطيات، هي من الجرائم العمدية التي ترتكز على القصد الجنائي بعنصريه العلم و الإرادة حيث ينتهي إلى علم الجاني فعل تعديه على نطاق الحق المحمي مع أن إرادته تتجه إلى إحداث فعل الإفساد أو التعطيل و الإعاقة و تحقق نتيجته، بعكس ما لو قام من هو مخوّل قانونا بالتعامل مع النظام بإحداث نتيجة الإفساد أو الإعاقة على سبيل الخطأ في التعامل مع النظام فإن المسؤولية منتفية عنه و الوصف الجرمي غير محقق في نشاطه لانتفاء القصد الجنائي[100]

المطلب الثالث : الاعتداء العمدي على المعطيات

---

[99] - حجازي مرجع سابق، ص 42

[100] - مسعود خثير مرجع سابق،ص 97.

بالنسبة للمشرع الجزائري نص على هذه الجريمة في المادة 394 مكرر 1 من قانون العقوبات "يعاقب بالحبس من ستة أشهر إلى ثلاث سنوات و بغرامة من 500.000دج إلى 2.000.000دج كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها"
كما نصت عليها المواد 03- 04- 08 من الاتفاقية الدولية للإجرام المعلوماتي، و نص عليها المشرع الفرنسي في المادة 3/323 من قانون العقوبات الحديث.
و يتحقق الركن المادي لهذه الجريمة بما يلي:

الفرع الاول: الركن المادي

السلوك المادي في هذه الجريمة منحصر في أحد هذه الأفعال (أو جميعها) الإدخال و المحو و التعديل، فبتوفر أحدها يقوم الركن المادي لهذه الجريمة الاعتداء العمدي أو القصدي على بيانات نظم معالجة بيانات التجارة الالكترونية، فالحاصل من وقوع أحد هذه الأفعال هو انطوائها على تلاعب في المعطيات التي يتضمنها نظام معالجة البيانات بإدخال معطيات جديدة أو محو أو تعديل لمعلومات أخرى، فالسلوك الإجرامي في هذه الجريمة إنما يرد على محل أو موضوع محدد و هو البيانات التي تمت معالجتها آليا و التي تحولت إلى رموز و إشارات أي عبارة عن معطيات متعلقة بمعلومة أي أن الجريمة تقع على المعطيات أي البيانات التي تمت معالجتها دون المعلومة ذاتها[101]، فالمعلومات التي لم تعالج بعد، أو لم تدخل إلى نظام معالجة البيانات و كذا البيانات التي دخلت النظام و لم يبدأ بمعالجتها أو التي خرجت من النظام فهي واقعة خارج إطار الجريمة[102]. و النص يحمي المعلومات المعالجة داخل النظام أو تلك التي في طريقها للمعالجة، و الفعل الجرمي الواقع على هذه المعطيات هو فعل الإدخال و المحور و تعديل البيانات المثبتة في النظام، و هو ما يمكن أنه يدخل في عداد ما يعرف بـــ القرصنة المعلوماتية، كما لا يشترط أن تقع أفعال الإدخال و المحو و التعديل بطريق مباشر بل يمكن أن يقع ذلك بطريق غير مباشر، كأن يحدث ذلك بوساطة طرف ثالث أو بالتحكم عن بعد[103].

---

[101] **Nicolas MATHEY, Le commerce électronique dans la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, Contrats Concurrence Consommation n° 10, Octobre 2004, Etude 13**

[102] - نفس المرجع ،ص 97،98.

[103] - آمال قارة ،مرجع سابق ، ص، مرجع سابق، 121.

و لعل تبيان الركن المادي لهذه الجريمة يوضحه تبيان صور السلوك الإجرامي التي سبق الإشار ة لها، الإدخال: L'Intervision ، المحو: L'effacement ، التعديل: Modification

01- فعل الإدخال:

يحدث عادة هذا الفعل من قبل من له مركز متنفّذ في النظام المعلوماتي و يتعامل معه أو من يكتسب آلية الدخول إليه و يقصد بفعل الإدخال إدخال بيانات في نظام المعالجة لم تكن موجودة من قبل، و يتم فعل الإدخال بغرض التعديل في البيانات القائمة مما يؤثر على صحتها بإضافة معطيات جديدة، و يقع فرض فعل الإدخال حين يتمكن حامل البطاقة الممغنطة الشرعي، التي تسحب بها النقود أكثر من رصيد حسابه الحقيقي، و تقع حتى من حاملها غير الشرعي عند سرقتها أو فقدها أو تزويرها[104].

كذلك من الصور العملية لفعل إدخال معلومات مصطنعة قيام مسؤول معلوماتي في مؤسسة تضم مستخدمين لا وجود لهم أو إبقاءهم بالرغم من عدم وجودهم، و لعل اصطناع المعلومات أو إضافتها هو العامل الأكثر سهولة في التنفيذ بالأخص في المنشآت ذات التعاملات المالية[105]، و حينئذ يكون المسؤول عن القسم المعلوماتي على علم أو هو الجاني، فمركزه يؤهله لارتكاب مثل هذا الفعل و يسهل عليه، كما يحدث في طرق اختلاس النقود عن طريق الغش المعلوماتي[106].

02- فعل المحو:

و يعرفه البعض بأن فعل المحو يتمثل في وقوع إتلاف أو أو محو للمعطيات لمعطيات متعلقة ببيانات التجارة الالكترونية التي يعالجها النظام آليا الموجودة في المواقع أوداخل الحاسب الآلي و يتحقق بإزالتها كلها أو إزالة جزء من المعطيات فقط، حيث يقع هذا الفعل بإزالة جزء من المعطيات المسجلة على الدعامة الموجودة داخل النظام أو تحطيم الدعامة أو نقل أو تخزين جزء من المعطيات إلى المنطقة الخاصة بالذاكرة و يتم عن طريق برامج غريبة تتلاعب في هذه المعطيات تتسبب بمحوها كليا

---

[104]-- نفس المرجع ،ص 121-122، انظر أيضا:

-Agathe LEPAGE, Libertés sur l'Internet et cybercriminalité : les apports au droit pénal de la loi pour la confiance dans l'économie numérique du 21 juin 2004, Droit pénal n° 12, Décembre 2004, Etude 18

[105] - مسعود خثير ، مرجع سابق ، 48.

[106] - حجازي 47.

أو جزئيا و أحيانا تتم بواسطة إستخدام القنبلة المعلوماتية الخاصة بالمعطيات أو برنامج الممحاة Gomme أو بواسطة فيروسات يصممها مجرم معلوماتي محترف ذو قدرة عالية في تقنية المعلومات بمن يعرفون بـــ " المجرمون ذو اللياقة البيضاء " [107]، بالإضافة إلى فيروسات حصان طروادة أو فيروس الدودة. و تستعمل هذه الآليات كذلك في فعل التعديل الذي نتعرف عليه فيما يلي:

03- فعل التعديل:

يختلف فعل التعديل عن فعل المحو و ذلك بأن سلوك الجاني في فعل التعديل إيجابي أي بقيامه بتغيير المعطيات الموجودة داخل النظام و استبدالها بمعطيات أخرى أو عن طريق التلاعب في البرنامج، و ذلك بإمداده بمعطيات مغايرة تؤدي لنتائج مغايرة عن تلك التي صمم البرنامج لأجلها. و أفعال الإدخال أو المحو أو التعديل وردت على سبيل الحصر، فأيما فعل عدا هذه الأفعال و لو تضمن اعتداء على هذه المعطيات الموجودة داخل نظام المعالجة الآلية للمعطيات فلا يخضع للتجريم بصورة الاعتداء العمدي على المعطيات، فلا يقع تحت طائلة التجريم فعل نسخ المعطيات أو فعل نقلها أو فعل التنسيق أو التقريب فيما بينها كون هذه الأفعال لا تنطوي على إدخال أو محو أو تعديل[108].

المطلب الرابع : المساس العمدي بالمعطيات خارج نظام المعالجة

كفل المشرع الجزائري الحماية الجزائية للمعطيات ذاتها بغض النظر عن كونها في إطار المعالجة أولا من خلال تجريم السلوكات التالية[109]:

المادة 394 مكرر 2 تستهدف حماية المعطيات في حذ ذاتها لأن المشرع لم يشترط أن تكون داخل المعالجة الآلية للمعطيات أو التي قد تمت معالجتها آليا إنما الحماية مقتصرة على المعطيات في أي موضع كانت مخزنة، سواء على أشرطة أو كانت مخزنة على أقراص أو مرسلة على طريق منظومة معلوماتية إذا ما كانت وسيلة لارتكاب أحد الجرائم المنصوص عليها في القسم السابع مكرر من قانون العقوبات.

أما المادة 394 مكرر 2/2 فإنه يجرم أفعال الحيازة، الإفشاء، النشر والاستعمال أيا كان الغرض من هذه الأفعال التي ترد على المعطيات المتحصل عليها من إحدى

---

[107] - حجازي مرجع سابق 52.

[108] - خثير مسعود ، مرجع سابق ، ص 99

[109] - آمال قارة ،مرجع سابق ، ص، مرجع سابق 123.

الجرائم الواردة في القسم السابع مكرر من قانون العقوبات بهدف المنافسة غير المشروعة، التحريض على الفسق (تجارة الجنس عن طريق المواقع الإباحية).

الفرع الأول: الركن المعنوي

هذه الجريمة لا تتطلب قصدا جنائيا خاصا كقصد الإضرار حيث الركن المادي يقوم بمجرد توافر فعل الإدخال أو المحور أو التعديل و بذلك فهذه الجريمة من الجرائم العمدية حيث يتوفر الركن المعنوي و يقوم بانصراف القصد الجنائي إلى أحد الأفعال السابقة فيجب أن تتجه إرادة الجاني إلى فعل الإدخال أو المحو أو التعديل ليقال بتوفر القصد الجنائي بعنصريه العلم و الإرادة، فيجب أن ينتهي إلى علم الجاني بأن نشاطه يترتب عليه التلاعب بالمعطيات و هو يشكل اعتداء على صاحب الحق المعطيات، أو من له السيطرة عليها، نشير إلى أن الضرر و إن كان يستحق نتيجة النشاط الإجرامي إلا أنه ليس عنصرا في الجريمة. فالجريمة تقوم دون توفر قصد الإضرار بالغير[110].

المطلب الخامس: العقوبات المقررة لهذه الجرائم في التشريع الجزائري والتشريعات المقارنة:

بالنسبة للاتفاقية الدولية للإجرام المعلوماتي فإنه و طبقا للمادة 13 من ذات الاتفاقية فإن العقوبات المقررة للإجرام المعلوماتي و لكي تكون ذات فعالية لابد و أن تكون رادعة و متضمنة لعقوبات سالبة للحرية، و التي هي عقوبات أصلية و عقوبات تكميلية، تطبق على الشخص الطبيعي، أما المادة 12 فتضمنت مبدأ مساءلة الشخص المعنوي بعقوبات موقعة عليه.

أما بالنسبة للمشرع الفرنسي، فإن تجربته في السياسة العقابية ضد الإجرام الالكتروني أو الجريمة المعلوماتية ظهرت منذ سنوات 1975 و أهم هذه المحاولات محاولة النائب Jaques Edofan[111] حول قانون الغش المعلومات، و بعد سنة و نصف من المناقشات أقر المشروع بعد تعديلات، و شكل الباب الثالث من الكتاب الثالث من القسم الثاني من قانون العقوبات الفرنسي و هو متعلق بالجنايات و الجنح أما الباب الثالث فهو متعلق بجرائم المعلوماتية ضمن المواد من 2/462 إلى 9/462 و مضمون المواد تجريم

---

[110]- مسعود خثير مرجع سابق 99.

[111]Philippe BOURE, Internet et la lutte contre la cybercriminalité, Revue Gazette du Palais, 23 janvier 2003 n° 23, P. 19

الدخول أو البقاء غير المشروع في نظام المعالجة الآلية للمعطيات. و يعتبر ظرفا مشددا للعقوبة في حالة محو أو تعديل المعطيات الموجودة فيه أو طرق معالجتها أو نقلها، و عاقبت هذه النصوص كل فعل عرقلة أو إفساد عمدا و دون مراعاة لحقوق الغير و عاقبت على جريمة التزوير و استعمال المستند المزور كما عاقب على جريمتي الشروع و الاتفاق الجنائي و التعديل الذي ورد في قانون 1994 فقد عدل من نص المادة 1/441 و أصبحت بموجب هذا التعديل من جريمة تزوير المستندات المعالجة آليا فقط إلى جريمة تزوير المستندات المعلوماتية و استعمالها و استقلت بالنص على جرائم الإعتداء على نظام المعالجة الآلية للمعطيات[112].

الفرع الاول : العقوبات الأصلية:

عاقب المشرع الفرنسي الشخص الطبيعي بعقوبات أصلية و أخرى تكميلية فبالنسبة للعقوبات الأصلية:

01- عقوبات الصورة البسيطة لجريمة الدخول أو البقاء غير المشروعين:

نصت المادة 1/323 عقوبات فرنسي على فعل الدخول أو البقاء غير المشروعين

لنظام معالجة البيانات أو في جزء منه بالحبس لمدة سنة و غرامة 100.000 فرنك فرنسي.

أما المشرع الجزائري فإن سياسته العقابية أخذت كذلك بنظام التدرج العقابي الذي يحدد الخطورة الإجرامية للاعتداء على تلك الحقوق، فالبنسبة للصورة البسيطة أي الدخول و البقاء غير المشروعين فالعقوبة المقررة هي 3 أشهر إلى سنة حبس و بغرامة تبدأ من 50.000دج إلى 100.000دج، فيما تضمنته المادة 394 مكرر عقوبات جزائري[113]

02- عقوبات الجريمة في صورتها المشددة:

إذا تعدى فعل الدخول أو البقاء إلى فعل محو أو تغيير في البيانات أو حدث تعييب لتشغيل النظام عند المشرع الفرنسي فالعقوبة تشدد و تقرر بالحبس لمدة سنتين و تصل الغرامة إلى 200.000 فرنك فرنسي.

---

[112]- حجازي مرجع سابق 19-20،انظر ايضا:

Nicolas MATHEY, Le commerce électronique dans la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique,Contrats Concurrence Consommation n° 10, Octobre 2004, Etude 13

[113]- آمال قارة ،مرجع سابق ، ص مرجع سابق 127، مسعود 100.

مثلما ضاعف المشرع الجزائري العقوبة في هذه الحالة لتكييفها كجريمة أو صورة مشددة للجريمة و قررها من ستة أشهر إلى سنتين و الغرامة من 50.000دج إلى 150.000دج فيما تضمنته المادة 394 مكرر 3/2.

كما رفع المشرع الفرنسي العقوبة في حالة إعاقة أو إفساد و تشغيل نظام معالجة البيانات إلى الحبس لمدة ثلاث سنوات و الغرامة 300.000 فرنك فرنسي طبقا لنص المادة 2/323 من قانون العقوبات الفرنسي الجديد و إلى نفس مدة الحبس رفعها المشرع الجزائري في المادة 394 مكرر 2 فقرر العقوبة من ستة أشهر إلى ثلاث سنوات و بغرامة من 500.000 دج إلى 2000.000دج بالإضافة إلى أنه عاقب على جريمة استخدام تلك المعطيات في ارتكاب الجرائم الماسة بالأنظمة المعلوماتية و حيازة أو إفساد أو نشر أو استعمال المعطيات المتحصل عليها من إحدى الجرائم الماسة بالأنظمة المعلوماتية بالحبس من شهرين إلى ثلاثة سنوات و غرامة من 1000.000دج إلى 5000.000دج.

الفرع الثاني: العقوبات التكميلية:

تعد العقوبات التكميلية من الأحكام المشتركة لجرائم الاعتداء على نظم معالجة البيانات ، وأورد المشرع الجزائري في نص المادة 394 مكرر 3 العقوبات التكميلية التي يحكم بها إلى جانب العقوبات الأصلية وتمثلت في:

المصادرة: تشمل الأجهزة، و البرامج و الوسائل المستخدمة في الفعل الجرمي الماس بالأنظمة المعلوماتية مع مراعاة حقوق الغير حسن النية .

إغلاق المواقع التي تكون محلا للجريمة الماسة بالأنظمة المعلوماتية.

إغلاق المحل إذا كانت الجريمة قد ارتكبت بعلم مالكه.

أما المشرع الفرنسي فتمثلت العقوبات التكميلية التي نص عليها فيما يلي:[114]

الحرمان من الحقوق السياسية و المدنية و العائلية لمدة لا تتجاوز خمس سنوات طبقا للمادة 26/131.

الحرمان من حق تولي الوظائف العامة أو أي نشاط مهني أو اجتماعي تكون الجريمة قد ارتكبت بسببه.

مصادرة الأشياء التي استخدمت في الجريمة أو الأشياء الناتجة عن الجريمة ذاتها.

[114] - علي عبد القادر القهوجي ، مرجع سابق ، ص مرجع سابق 124-125.

غلق المؤسسة أو المؤسسات التي ساهمت في ارتكاب الجريمة لمدة لا تتجاوز خمس سنوات.

الاستبعاد من التعامل في الأسواق العامة لمدة لا تتجاوز 05 سنوات.

الحرمان من إصدار الصكوك لمدة لا تتجاوز 05 سنوات

نشر الحكم أو تعليقه طبقا للشروط المنصوص عليها في المادة 35/131.

الفرع الثالث : عقوبات الشخص المعنوي

مبدأ مساءلة الشخص المعنوي بقصد مساءلته عن هذه الجرائم بصفته فاعلا أصليا أو شريكا أو متدخلا كما يسأل عن الجريمة التامة أو الشروع فيها بشرط أن تكون الجريمة قد ارتكبت لحساب الشخص المعنوي بواسطة أحد أعضائه أو ممثليه و نصت المادة 12 من الاتفاقية الدولية للإجرام المعلوماتي على هذا المبدأ [115] كما نصت على ذلك المادة 2/122 عقوبات فرنسي[116].

كما أن مسؤولية الشخص المعنوي الجنائية لا تستبعد مسؤولية الأشخاص الطبيعيين الجنائية بصفتهم فاعلين أو شركاء أو متدخلين في نفس الجريمة. المادة 2/121 فقرة 3.

أما العقوبات التي قررها المشرع الجزائري فجاءت عند تطرقه في المادة 18 مكرر من القانون 15/04 المتضمن قانون العقوبات لمبدأ المساءلة الشخص المعنوي و قد نصت المادة على أن:

العقوبات المطبقة على الشخص المعنوي في مواد الجنايات و الجنح هي:

الغرامة التي تساوي من مرة إلى 05 مرات الحد الأقصى للغرامة المقدرة لشخص الطبيعي في القانون الذي يعاقب على الجريمة.

واحدة أو أكثر من العقوبات التالية:

حل الشخص المعنوي

غلق المؤسسة أو فرع من فروعها لمدة لا تتجاوز 05 سنوات

---

[115] - آمال قارة ،مرجع سابق ، ص مرجع سابق 129.

[116] - علي عبد القادر القهوجي ، مرجع سابق ، ص مرجع سابق ،126، كذلك
Christophe CARON, Le risque de confusion, élément constitutif de la contrefaçonCommunication Commerce électronique n° 2, Février 2007, comm. 21

المنع من مزاولة نشاط أو عدة أنشطة مهنية أو اجتماعية بشكل مباشر أو غير مباشر نهائيا لمدة لا تتجاوز 05 سنوات.

مصادرة الشيء الذي استعمل في ارتكاب الجريمة أو نتج عنها.

نشر أو تعليق حكم الإدانة

الوضع تحت الحراسة القضائية لمدة لا تتجاوز 05 سنوات و تنصب الحراسة على ممارس النشاط الذي أدى إلى الجريمة أو الذي ارتكبت الجريمة بمناسبته.

أما العقوبات التي أوقعها المشرع الفرنسي على الشخص المعنوي فهي الواردة في المادة 6/323 وفقا للشروط الواردة في المادة 2/121[117]:

الغرامة المقدرة بخمسة أمثال الغرامة التي يحكم بها على الشخص الطبيعي كحد أقصى الرقابة القضائية

غلق المنشأ

الاستبعاد من التعامل في الأسواق العامة

الحرمان من الاكتتاب العام في الادخار

الحرمان من مزاولة النشاط المهني بسببه أو بمناسبته ارتكبت الجريمة.

الفرع الرابع : الشروع في الجريمة

قيد المشرع الجزائري عموم المبدأ الذي يقضي بعدم العقاب على الشروع في الجنح بنص خاص ضمنه إمكانية العقاب على الشروع في هذه الجرائم أي الماسة بالأنظمة المعلوماتية، و هو ما تضمنته المادة 7/394 مكرر 7 من قانون العقوبات و نصت على أنه " يعاقب على الشروع في ارتكاب الجنح المنصوص عليها في هذا القسم بالعقوبات المقررة للجنحة ذاتها "[118]

و هذا نهج ردعي قد اتجه إليه المشرع لإحاطة نظام هذه التجارة بحماية نوعية لأجل دعمها و نماءها حسب رأينا ثم لخطورة مثل هذا النوع من الجرائم.

و يقابل هذا النص ما أورده المشرع الفرنسي في المادة 7/323 من قانون العقوبات الجديد.

الفرع الخامس : الاتفاق الجنائي

---

[117] - المرجع نفسه 126/125.

[118] -آمال قارة ،مرجع سابق ، ص مرجع سابق 132.

لأجل تقرير حماية متقدمة ووقائية للنظم المعلوماتية عموما ولنظام التجارة الالكترونية خصوصا خرج المشرع الفرنسي عن القواعد العامة في العقاب على الجرائم إذ نقض هذه القواعد بأن العقاب لا يقع و لا يقرر إلا على الجرائم التامة أو تلك التي تقف عند الشروع أو المحاولة، أما الأعمال التحضيرية التي تسبق البدء في التنفيذ فلا عقاب عليها كقاعدة عامة.

ونص المادة 4/323 يعد استثناءا من القاعدة العامة أو هو النص الخاص الذي يقيّد العام فقد عاقبت على مساهمة أكثر من شخص في ارتكاب أفعال مادية تحضيرية تهدف إلى ارتكاب إحدى الجرائم المنصوص عليها في المواد 1/323 إلى 3/323[119].

أما المشرع الجزائري فقد عاقب على الاتفاق الجنائي بنص المادة 394 مكرر 5 حين نص على أن " كل مشارك في مجموعة أو في اتفاق تألف بغرض الإعداد لجريمة أو أكثر من الجرائم المنصوص عليها في هذا القسم و كان هذا التحضير مجسدا بفعل أو عدة أفعال مادية، يعاقب بالعقوبات المقررة للجريمة ذاتها ".

و نخلص إلى أن نحصي الشروط التي وضعها المشرع الجزائري لأجل العقاب على جريمة الاتفاق الجنائي هي:[120]

- وجود مجموعة أشخاص أو انعقاد اتفاق فالأعمال التحضيرية المرتكبة من طرف شخص منفرد لا يشملها هذا النص أي (الاشتراك في الاتفاقية)
- استهداف الإعداد لجريمة ماسة بالأنظمة المعلوماتية (القصد الجنائي)
- تجسيد الأعمال التحضيرية بفعل مادي أو عدة أفعال.

و قد نصت على هذه العقوبة المادة 11 من الاتفاقية الدولية للإجرام المعلوماتي.

المبحث الثاني :الحماية الجنائية للبيانات الشخصية و الاسمية

من أهم المخاوف التي تعترض نمو التجارة الالكترونية و قيام نظام متقن لها و متداول، و لأجل ذلك اهتمت التشريعات الحديثة بتوفير حماية لقواعد البيانات التي تتعلق بيانات اسمية للمتعاملين في هذا الميدان التجاري[121].

فوضعت مجموعة من التشريعات المقارنة مجموعة ضوابط و ضمانات استهدفت خلق رقابة فعالة على إنشاء نظم المعلومات و كيفية استخدامها سواء أكانت

---

[119] - علي عبد القادر القهوجي ، مرجع سابق ، ص مرجع سابق 127-128.
[120] - آمال قارة ،مرجع سابق ، ص مرجع سابق 131.
[121] - مدحت رمضان عبد الحليم ، مرجع سابق ، ص109.

هذه الاستعمالات و الاستخدامات تتعلق بالنشاط الحكومي أو بالقطاع الخاص أو بالأفراد لأجل حماية الحريات العامة و بالأخص الحريات الشخصية[122] .

ومن المعلوم أنه يتم المعاملات التجارية الالكترونية أنها تتطلب تبادل بيانات تتعلق بالعملاء قد يكون من هؤلاء العملاء المتعاملين بالمشروعات أي بياناتها متعلقة بالموظفين و القائمين على الإدارة، هذا الأمر دفع إلى ظهور إشكالات متعلقة بتوفير حماية قانونية للمتعاملين بهذه الرابطة التعاقدية التقنية و بخاصة الطرف الأضعف فيها ألا و هو المستهلك فيما يتعلق بحمايته من الاطلاع على بياناته الاسمية أو الشخصية التي يدلي بها في عملية إبرام العقد.[123]

تقتضي المعاملة التجارية الالكترونية تبادل البيانات الالكترونية تبادل البيانات الالكترونية و استخدام الوثائق الالكترونية عن طريق مورد الخدمات الالكترونية و قد تتعرض هذه المعاملة التجارية الالكترونية لاعتداء فيما يتعلق في التعامل في هذه البيانات أو جريمة التصريح عمدا بمعطيات خاطئة.[124]

و البيانات التي تتعلق بالمعاملة التجارية الالكترونية يتعين المحافظة على سريتها و خصوصيتها عن طريق وسائل أمان تتسم بالسرية و القدرة على حماية البيانات و الحفاظ على سريتها ومدى حرية تداولها و سلامتها.[125]

المطلب الأول: صور الاعتداءات الواقعة على للبيانات الشخصية والاسمية

استهدف المشرع الفرنسي تأكيد حماية حقوق و حريات المواطنين في مواجهة تطور تكنولوجيا المعلومات من خلال تلك السلطة التي أعطاها اللجنة القومية للمعلومات و الحريات CNTL [126].

أو بالقانون المتعلق بالمعلوماتية و الحريات الصادر بتاريخ 1978/01/06 أو حتى فأكد عليه في التعديل الجديد لقانون العقوبات الفرنسي في الفصل و أكد المشرع الفرنسي هذه الحماية في القانون الجديد للعقوبات في الفصل الخاص بحماية الشخصية و

---

[122] **Éric A. CAPRIOLI, Loi du 6 août 2004. Commerce à distance sur l'Internet et protection des données à caractère personnel,** Revue **Communication Commerce électronique n° 2, Février 2005, Etude 7**

[123] - مدحت رمضان عبد الحليم ، مرجع سابق ، ص75، حجازي 56.

[124] - هدى حامد قشقوش ، مرجع سابق ، ص حامد ح ح ت إ 36.

[125] - حجازي 56-57.

[126] - للإطلاع أكثر على هذه مهام هذه اللجنة أنظر حجازي 70-72.

تناولت الجرائم المتعلقة بالبيانات الاسمية و الأحكام الخاصة و العقاب في المواد 226-16، 226-24 و 226-31 و يتعلق الأمر بالجرائم التالية[127].

م 226- 16جريمة عدم اتخاذ الإجراءات الأولية لإجراء معالجة البيانات

م 226- 17 جريمة المعالجة غير المشروعة للبيانات

م 226- 18 جريمة المعالجة غير المشروعة للبيانات

م 226- 19 جريمة تسجيل و حفظ بيانات شخصية أو بيانات تتعلق بالماضي لأشخاص مصنفين

م 226- 22 إفشاء البيانات الاسمية بما يضر بصاحب الشأن

كما ضمن المشرع المادة 432- 9 من قانون القانون الجديد توفير حماية للمراسلات التي تتم بطريق وسائل الاتصالات

الفرع الأول : جريمة التقاعس عن الإجراءات المبدئية لمعالجة البيانات:

نص المشرع الفرنسي على هذه الجريمة في المادة 226- 16 و التي كانت تضمنتها المادة 41 من قانون 1978 و استقراء نص الأخيرة يجعل من معالجة البيانات الاسمية من تلك التي تمس الحقوق و الحريات العامة، و عند انتقاء المساس بهذه الحقوق يكتفي بإخطار اللجنة القومية للمعلوماتية و الحريات[128].

و عند صدور القانون الجديد للعقوبات نص على هذه الجريمة في المادة 226- 16 حيث عاقب كل من يقوم _ و لو بإهمال _ بمعالجة إلكترونية للبيانات الاسمية دون مراعاة للإجراءات الأولية للقيام بها بالحبس لمدة ثلاث سنوات و بغرامة 300.000 فرنك و ينطح من هذا النص أن ألفاظه جاءت عامة بعدم مراعاة الإجراءات الأولية المحددة أي أنه لم يحل مثل المادة 41 من قانون 1978 إلى نصوص المادتين 15- 16 من نفس القانون.

فالركن المادي في هذا الجريمة يقوم نص عليها في القانون كما يعاقب بوصفه فاعل أصلي في الجريمة كل من أمر بفعل المعالجة حسب القواعد العامة لمسؤولية الفاعل في القانون الجنائي أما الركن المعنوي فإنه يستوي أن يأخذ فيه صوره العمد [129]

[127] - مدحت رمضان عبد الحليم ، مرجع سابق ، ص90/ حجازي 69.
[128] - للإطلاع على هذه اللجنة أنظر حجازي 70- 71، فوزي أو صديق 49 و ما بعدها.
[129] - حجازي 73.

أو الخطأ أي أنه يعاقب بنفس العقوبة الحبس و الغرامة سواء أخذ الركن المعنوي صوره القصد الجنائي أو الخطأ غير العمدي[130].

الفرع الثاني : جريمة عدم اتخاذ الحيطة في حماية البيانات المعالجة

نصت على هذه الجريمة المادة 226- 17 من قانون العقوبات الفرنسي بأنها "يعاقب بالحبس لمدة خمس سنوات و بغرامة 200.000 فرنك من يجرى أو أمر بإجراء معالجة إلكترونية للبيانات الاسمية دون اتخاذ الاحتياجات الملائمة لحماية هذه البيانات، و خصوصا الحيوية دون تشويهها أو إتلافها أو إطلاع غير المصرح له بذلك عليها[131].

و يتمثل الركن المادي لهذه الجريمة في عدم اتخاذ الاحتياجات اللازمة لفعل المعالجة الالكترونية للبيانات الاسمية _ أو الأمر بذلك _ حسب الأصول العلمية لحماية هذه البيانات و هذا ضد أي فعل من شأنه تشويه أو إتلاف البيانات أو إطلاع الغير عليها.[132]

أما الركن المعنوي في هذه الجريمة فيستوي كذلك فيه القصد الجنائي أي الخطأ غير العمدي أي أن عقوبة الفعل في صورتين بطريق العمد أو الخطأ هي متماثلة مع إعطاء القاضي السلطة التقديرية في تقرير العقوبة[133].

الفرع الثالث : جريمة المعالجة غير المشروعة للبيانات

وجاء النص على هذه الجريمة في المادة 226- 18 من قانون العقوبات على أنه يعاقب كل من يقوم بجمع معلومات خفية أو بصورة غير مشروعة أو معالجة بيانات اسمية تتعلق شخص طبيعي على من اعتراضه و كان الاعتراض يقوم على الرغم من اعتراضه و كان الاعتراض يقوم على أسباب مشروعة بالحبس لمدة خمس سنوات و غرامة 200.000فرنك.

و إذا كانت معالجة البيانات الاسمية لأغراض تتعلق بالأبحاث في حالات الصحة عوقب الجاني بذات العقوبات:

إذا لم يخطر أصحاب الشأن بحقهم في الإطلاع عليها و تصحيحها و الاعتراض عليها و بطبيعة البيانات و سيتلقاها إذا كان هناك اعتراض لن صاحب الشأن أو إذا كان القانون يقرر ضرورة توافر موافقة صريحة و واضحة من صاحب الشأن، أو إذا تعلق

---

[130] - حجازي 73.
[131] - مدحت رمضان عبد الحليم ، مرجع سابق ، صعبد الحليم ، مرجع سابق ، ص95، حجازي 73.
[132] حجازي 74، مدحت 96.
[133] - حجازي 74.

الأمر بمتوفى اعترض قبل وفاته على معالجة البيانات [134] و يأخذ الركن المادي لهذه الجريمة بتنوع صوب فعل الجريمة ذاتها.

فقد تتحقق صورة وقوع احتيال أو غش أو ما عبر عن المشرع في النص جمع المعلومات بطريقة خفية أو بصورة غير مشروعة و إن كان جانب من الفقه الفرنسي[135] يعلق على عبارة مبرارات مشروعة des raisons légitimes أنه مصطلح مطاط غير دقيقة و غير مضبوطة فإن جانب آخر أشار إلى ضرورة وجود تناسب بين المعلومات و من الهدف من تسجيلها لتحديد تلك المبررات التي تحكم اعتراض الشخص على فعل المعالجة[136].

أما الفقرة الثانية فسلمت صورا أخرى للركن المادي حيث اعتدت لقيام الركن المادي فيما بقي من صور عدم إطلاع الأشخاص الطبيعيين على حقهم في الإطلاع على الطبيعية المتعلقة بهم، أو معالجة بيانات متعلقة بمتوفى اعترض قبل وفاته معالجة البيانات حماية لهذه البيانات الشخصية.

عموما يتحقق الركن المادي للجريمة إذا تمت المعالجة الآلية للبيانات لغير الأغراض الطبيعية أو إذا _ و لو التزم بالغرض من المعالجة _ لم يخطر أصحاب الشأن بحقهم في الإطلاع و التصحيح و الاعتراض [137] أو قام بالمعالجة بالرغم من اعتراض صاحب الشأن و عدم وجود موافقة صريحة من الأخير[138].

و الركن المعنوي لهذه الجريمة فهو القصد الجنائي أي أنها لا تقع بطريق الخطأ بل يجب توافر علم الجاني بأن هذه الأفعال معاقب عليها جنائيا و تنصرف إرادته إلى إتيان هذه الأفعال.[139]

الفرع الرابع : جريمة حفظ البيانات شخصية

أورد المشرع النص على عقوبة هذه الجريمة في المادة 226- 19 من قانون العقوبات الجديد حيث أورد صورتين للركن المادي حيث تعلقت الأولى بمعالجة بيانات اسمية خاصة بأشخاص سبق تصنيفهم تظهر بصورة مباشرة أو غير مباشرة أصولهم العرقية أو معتقداتهم الفلسفية أو انتماءاتهم السياسية أو الدينية أو النقابية [140]و يتمثل فعل

---

[134] - مدحت رمضان عبد الحليم ، مرجع سابق ، ص96- 97.
[135] - مدحت رمضان عبد الحليم ، مرجع سابق ، ص97.
[136] - حجازي 76.
[137] - مدحت رمضان عبد الحليم ، مرجع سابق ، ص99.
[138] - مدحت رمضان عبد الحليم ، مرجع سابق ، ص 100.
[139] - حجازي 78.
[140] - حجازي 78- 79.

هذه الجريمة في وضع البيانات و حفظها دون موافقة من صاحبها، إذ أن الموافقة الصريحة لصاحب الشأن تمنع العقوبة المقررة، و يفرع الحماية من مضمونها[141].

أما الصورة الثانية لركنها المادي فتتمثل في معالجة بيانات اسمية لأشخاص سبق تصنيفهم تظهر جرائم الشخص التي ارتكبها و ما صدر في حقه من أحكام إدانة أو تدابير متخذة ضده أو يأمر بمعالجة هذه البيانات.

و السبب في رأي البعض في تجريم هذه الأفعال هو استبعاد كل تميز مؤسس على العرق أو الدين أو الائتمان السياسي بما يهدد مبدأ المساواة استهدافا لحماية حرية الفكر و الرأي و التعبير و العقيدة، فيخطر معالجة البيانات المتعلقة بالحياة الخاصة[142].

و يحظر _ على غير الجهات القضائية أو السلطات العامة المخولة قانونا و في حدود اختصاصاتها القانونية_ معالجة مثل هذه البيانات آليا حماية لسمعة و اعتبار الشخص.

أما الركن المعنوي فيتحقق بتوافر القصد الجنائي العام بعنصريه العلم و الإرادة أي أن يعلم الجاني يعالج بيانات خاصة دور موافقة صاحبها سواء تعلقت هذه البيانات بالائتمان العقيدي أو الفلسفي أو الميول السياسي أو النقابي و تنصرف إرادته إلى إحداث النتيجة بسلوكه الإجرامي[143].

بأن يعاقب بالحبس لمدة خمس سنوات و بغرامة 200.000 فرنك كل من قام بعملية وضع أو حفظ ذاكرة الكترونية دون موافقة صريحة من قبل صاحب الشأن بيانات تظهر بصورة مباشرة أو غير مباشرة أصوله العرقية أو معتقداته السياسية أو الفلسفية أو الدينية أو انتمائته النقابية أو تتعلق بأخلاقه، كما يعاقب بذات العقوبات من يقوم في غير الحالات، التي يقررها القانون بوضع أو حفظ بيانات اسمية في ذاكرة الكترونية تتعلق بالجرائم أو أحكام الإدانة أو التدابير[144]

الفرع الخامس : جريمة تجاوز الوقت المصرح به في الإعلان السابق أو موقف للطلب

---

[141] - مدحت رمضان عبد الحليم ، مرجع سابق ، ص101.

[142] **Agathe LEPAGE, Réflexions de droit pénal sur la loi du 6 août 2004 relative à la protection des personnes à l'égard des traitements de données à caractère personnel,** Revue **Droit pénal n° 3, Mars 2005, Etude 5**

[143] - حجازي 81.

[144] - مدحت رمضان عبد الحليم ، مرجع سابق ، ص100.

جاء النص على هذه الجريمة في المادة 226–20 بالعقوبة المقررة بالحبس لمدة ثلاث سنوات و بغرامة 300.000 فرنك كل شخص قام دون موافقة اللجنة القومية و الحريات بحفظ معلومات إسمية بما يجاوز الوقت المحدد في طلب الموافقة أو الإخطار السابق على عملية المعالجة.

عامل الوقت في المعاملة الالكترونية عامل محوري حيث يمكن حفظ بيانات متعلقة بشخص في ظرف وقت قياسي و تحد كل من متعهد الوصول و متعهد الإيواء، و ناقل المعلومات و مورد المعلومات و مورد الرسائل الفنية و متعهد الخدمات هم من الأشخاص المهنيين المعهود لهم بمعالجة البيانات الاسمية في معاملات التجارة الالكترونية و هم مسئولون جنائيا كل حسب مساهمتهم في السلوك الإجرامي المتعلق بتجاوز حفظ البيانات الاسمية مدة تزيد عما هو مقرر لها قانونا[145].

حيث تقوم إمكانية تسجيل أو ضبط بيانات اسمية خارج الوقت المخصص لمعالجتها، فالوقت فقد بكل جزئياته في مثل هذه العمليات ضمن ضوابط تخزين و معالجة المعلومات الشخصية و الاسمية توقيت عملية التخزين لتلك المعلومات و قد عالجت المادة 28 من قانون المعلوماتية و الحريات على أنه لا يجوز الاحتفاظ بالمعلومات الاسمية إلا للمدة المحددة في طلب إقامة نظم المعلومات أو لمدة تزيد على المدة اللازمة لتحقيق الغرض من تجميع البيانات و احتياجات البرنامج، إلا إذا سمحت اللجنة القومية للمعلوماتية و الحريات بالاحتفاظ بهذه المعلومات أكثر من المدة المحددة[146].

و من المعلوم أن اللجنة الوطنية للمعلوماتية و الحريات تتمتع بسلطة رقابية يمكنها من أن تمارس حصر و متابعة المخالفات المتعلقة بالمعالجات الآلية للمعلومات الاسمية الأمر الذي يجعل فيها سلطة عقابية بشروط معينة.[147]

---

[145]- **Nathalie DREYFUS, De la responsabilité des intermédiaires techniques : contrefaçon ou responsabilité civile ? Revue Communication Commerce électronique n° 1, Janvier 2007, Alerte 1**

[146] - حجازي 81.

[147] - حدد المجلس الدستوري الفرنسي شروط الاعتراف بالعقوبات التي توقعها اللجنة الوطنية للمعلوماتية و الحرية هي :
- ضرورة احترام مبدأ شرعية الجرائم و العقوبات
- ضرورة احترام مبدأ العقوبة
- ضرورة احترام مبدأ عدم رجعية لقوانين العقوبات.
- ضرورة احترام حقوق الدفاع
للإطلاع أكثر، أنظر حسام أحمد حسام طه تمام ، مرجع سابق ، ص 122- 125.

و يقوم الركن المادي لهذه الجريمة إذا احتفظ الجاني بما تمت معالجته آلية فوق المدة المطلوبة للحفظ و المحددة في القانون و تجاوزها، حيث يؤكد المشرع أن البيانات الاسمية لا يمكن أن تحفظ لمدة غير محددة لما يتوقع أنه تمس به سمعة الشخص لتعلقها بحياته الخاصة و لو كانت متعلقة بأمور بسيطة.

أما الركن المعنوي في هذه الجريمة يقوم عندما تنصرف [148] إرادة الجاني إلى الاحتفاظ بالمعلومات مدة تزيد عن المدة المحددة، و انتهى إلى علمه مخالفته بهذا الفعل للقانون و مع ذلك تنصرف إرادته لهذا الفعل أي أن الركن المعنوي يقوم على القصد الجنائي العام بعنصريه العلم و الإرادة[149].

الفرع السادس : جريمة تغير الغرض من جمع البيانات الاسمية

يفترض أن يكون هناك تناسب بين تسجيل البيانات الشخصية المعالجة آليا و بين الغرض الذي تمت معالجتها لأجله الذي يكون محددا في طلب الموافقة على معالجة البيانات و قد احتاط المشرع الفرنسي من أي استخدام غير مشروع من قبل حائز البيانات الاسمية، أي باستخدامها في غير الغرض الذي خصصت له.[150]

و هذا الاحتياط تجلى في العقوبة التي قررها المشرع في المادة التي نصت على أن "يعاقب بالحبس لمدة خمس سنوات و غرامة 200.000 فرنك كل من يحوز بيانات اسمية بمناسبة تسجيلها أو فهرستها أو نقلها أو تحت أي شكل آخر من أشكال المعالجة، و قام بتغير الغرض فيها المحدد بالنص القانوني أو اللائحة المنظمة بالموافقة على المعالجة أو بقرار اللجنة القومية للمعلوماتية و الحريات بالتصريح بمعالجة البيانات لأغراض الأبحاث الطبية أو بالإخطار المسبق لإجراء المعالجة"[151].

الفرع السابع : جريمة إفشاء البيانات الاسمية على نحو يضر بصاحب الشأن

عاقبت المادة 226- 21 من قانون العقوبات الفرنسي "بالحبس لمدة سنة و بغرامة 100.000 فرنك على كل فعل يرتكبه شخص قام بالكشف عن بيانات إسمية، بمناسبة تسجيل أو فهرست أو نقل أو أي شكل من أشكال معالجة البيانات الاسمية و التي يترتب على كشفها الاعتداء على اعتبار صاحب الشأن أو حرمة حياته الخاصة. عن هذه المعلومات دون التصريح بذلك من صاحب الشأن، للغير الذي لا توجد له أي

---

[148] - حجازي 82، مدحت رمضان عبد الحليم ، مرجع سابق ، ص102.
[149] - حجازي 82.
[150] - مدحت رمضان عبد الحليم ، مرجع سابق ، ص103.
[151] - مدحت رمضان عبد الحليم ، مرجع سابق ، ص103، حجازي 84.

صفة في تلقي هذه المعلومات، و تكون العقوبات، الغرامة 50.000 فرنك إذا وقعت الجريمة السابقة نتيجة عدم الاحتياط أو الإهمال".[152]

تطور رسائل الاتصال و تضاعف الحاجة إلى استخدام شبكة الإنترنيت (المعلوماتية) بقدر ما سهل آلية الحصول على المعلومات و العامل معها بقدر ما شكل تهديدا للعديد من المراكز القانونية لكل الأشخاص (معنويين كانوا طبيعيين)[153].

حيث أدى ذلك إلى ظهور انتهاكات من نوع جديد بسبب التقنيات الفنية للمتسللين الذين يسعون إلى حصول على معلومات شخصية باستراقها من البريد الالكتروني أو المحادثات الخاصة و هذا الفعل يهدد حرمة الحياة الخاصة حيث للمحادثات الشخصية حرية لا يجوز انتهاكه[154]ا.

و قد اجتهد المشرعون في تجريم تسجيل الأحاديث الشخصية أو مراقبتها بأية وسيلة.

و قد تكون هامة و في غاية السرية و من شأن إفشائها أن تلحق بأصحابها أضرارا و الذي نلاحظ في هذا النص هو أن المشرع الفرنسي لم يعين أي نوع من الضرر مما يجعل للقاضي الجزائي سلطة تقديرية أوسع في تكييف الضرر بصورتيه المادي أو المعنوي في إطار ما يمس بالاعتبار الشخصي أو حرمة الحياة الخاصة بشرط انتقاء تصريح من قبل صاحب الشأن.

هذه الجريمة لا يشكل الفعل المادي فيها اختراقا لشبكة المعلوماتية و لا قرصنة تقع على البيانات الشخصية المعالجة، بل يقع هذا الفعل الإجرامي من قبل الشخص المؤهل بمباشر هذه الأعمال سواء تمثل في التسجيل أو الفهرسة أو نقل هذه البيانات أو شكل من أشكال المعالجة الآلية للبيانات الاسمية[155].

---

[152] - 85.

[153] **Antoine LATREILLE, LA PROTECTION JURIDIQUE DES BASES DE DONNEES ELECTRONIQUES, Revue petites affiches, Droit de la communication, 28 avril 1995 n° 51, P. 14**

[154] - حسام أحمد حسام طه تمام ، مرجع سابق ، ص 318،انظر أيضا : **LATREILLE Antoine ....., P. 14**

[155] **Antoine LATREILLE ....., P. 14**

و يتمثل ركنها المادي في فعل الإفشاء أن يقوم الجاني بإفضاءها لشخص آخر لا صفة له في تلقي هذه البيانات و ما تعلق بها من معلومات[156].

جدير بالذكر أنه يجب التفرقة بين صورتان متشابهتان لذات الفعل و هو ما يمكن يشبه بجريمة إفشاء الأسرار المهنية التي نص عليها المشرع الفرنسي في المادة 324 و التي هي فعلا متعلقة بصورة أعمق بمعاملات التجارة الالكترونية الفارق بينهما أن جريمة إفشاء البيانات الاسمية قد ينطوي على بيانات لا تعد من قبيل الأسرار و هي بالتالي أوسع نطاقا من جريمة إفشاء الأسرار[157].

و إن كان الركن المادي لهذه الجريمة له صورتان يفرق بينهما الركن المعنوي و تبعا لكل صورة قرر المشرع عقوبة تتلائم و الفعل الإجرامي كيفما توفر القصد الجنائي العام بعنصريه العلم و الإرادة أي أنه يعلم الجاني أنه بإفضاءه إلى الغير بيانات بمناسبة تسجيله لها أو فهرستها أو نقلها أو بأي شكل من أشكال المعالجة دون موافقة صاحبها يرتكب فعلا مخالفا للقانون و يعاقبه عليه و تتجه مع هذا العلم إرادته إلى فعل هذا السلوك الجرمي و يتوقع نتيجة الفعل و يريدها و عند توفر هذه الصورة فإن المشرع قرر العقوبة المشددة لها[158] بالحبس لمدة سنة و بغرامة 100.000 فرنك.

و خفض هذه العقوبة في الصورة الثانية أي التي ينفي فيها في الركن المعنوي فيها إرادة الجاني لإحداث نتيجة الفعل الجرمي أي ينتفي فيها القصد الجنائي فقط يكون الموظف أو المكلف بالمعالجة قد أفشى هذه البيانات بسبب عدم الاحتياط أو الإهمال فقد العقوبة و أنزلها إلى الغرامة بـــ 50.000 فرنك حصرا لأن الفعل حدث مع عدم وجود إرادة آثمة استهدفت نتيجته، و هذا النص من شأنه أن يحفظ للتجارة الالكترونية و يحفظ لمعاملاتها جانبا من الثقة و آمان أكبر و توفير حماية خاصة بالطرف الأضعف في علاقتها التعاقدية ألا و هو المستهلك.

كما أن جريمة إنشاء البيانات الاسمية و الشخصية عادة ما تتعلق بالأشخاص الطبيعيين و كذلك أن مجال البيانات التي أفشيت هي متنوعة من حيث المجالات (شخصية، عائلية، مهنية، سياسية، عقائدية، فكرية..) وقد توصف بأنها أسرار كما يمكن أن لا تكون من قبيل الأسرا ر كما سلفنا لكن جريمة إفشاء الأسرار المهنية هي أكثر

---

[156] - و إن كان البعض يرى بأنه من الصعوبة بمكان تحديد من له هذه الصفة من الناحية النظرية عدا أنه يتضمن طلب الترخيص بمعالجة البيانات يتضمن بيان الأشخاص الذين تعد البيانات لمصلحتهم، مدحت رمضان عبد الحليم ، مرجع سابق ، ص105.

[157] - مدحت رمضان عبد الحليم ، مرجع سابق ، ص104.

[158] - حجازي 90.

تدقيقا حيث تتعلق بأشخاص معنويين و تخص مجالات صناعية أو تجارية أو مهنية حيث تتماثل[159].

و تتماثل الجرعات في فعل إفشاء معلومات قد تكون هامة و سرية للغاية من شأن إذاعتها أو إفضاءها أن يلحق بأصحابها كبير الضرر بالأخص إذا تلقاها ظرف منافس، و المعلومة في دنيا الأعمال مصدر الثروة.

و نصت المادة 418 من قانون العقوبات الفرنسي على أنه كل مدير أو مثل مدير أو عامل يطلع أو يحاول إطلاع الأجانب أو الفرنسيين المقيمين في الخارج على أسرار المصنع الذي يعمل فيه سيعاقب بالسجن لمدة تتراوح بين سنتين إلى خمس سنوات و بالغرامة من 18.000 فرنك إلى 120.000 فرنك فرنسي.

و الملاحظ على النص أنه لم يشر إلى ماهية هذه المعلومات و لا الكيفية التي تكون عليها هل هي من قبيل المحررات أو المخططات أو النسب و الإحصائيات أو البرامج أو البيانات الرقمية مما يجعلنا نأخذ بالتعريف الموسع لماهية الأسرار.

و قد قدم القضاء و الفقه معايير عدة لحصر هذه الأسرار هي:[160]

- أن يكون للسر قيمة تجارية
- أن يكون للسر صفة صناعية
- أن يكون عنصرا من عناصر الصناعة
- لا يشترط أن يكون السر متعلقا بشيء جديد أو..... لكن قد يتعلق بالبرامج.

و هذا يعني أن الفقه و القضاء كلاهما لم يستبعد بل أكد إمكانية أن تكون هذه الأسرار من قبيل المعلومات و البيانات المعالجة آليا مادام هذا السر تستخدمه المؤسسة تستأثر به و من شأن إفشاءه إلحاق الضرر بها.

الفرع الثامن : جريمة التصنت على المراسلات

نص المشرع الفرنسي على هذه الجريمة في المادة 9/432 و قد سبق و أن نص على تلك الحماية المقرر للمراسلات في القانون الذي صدر في يوليو 1991.

و عاقبت المادة 9/432 كل شخص عام أو مكلف بخدمة عامة بالحبس مدة 3 سنوات و غرامة 300.000 فرنك إذا ما قام عند مباشرته لعمله أو بمناسبته بالأمر أو

---

[159] **Antoine LATREILLE....., P. 14**

[160] - حسام أحمد حسام طه تمام ، مرجع سابق ، ص 326.

التسهيل أو القيام، في غير الحالات المقررة قانونا باختلاس أو إلغاء أو فض المراسلات و كشف محتواها[161].

كما جرمت الفقرة الثانية من نفس المادة كل شخص عام أو مكلف بخدمة عامة أو بأعمال استغلال خدمة الاتصالات أو بأعمال تقديم خدمة الاتصالات بالحبس مدة 3 سنوات و غرامة 300.000 إذا قام عند مباشرته لعمله بالأمر أو التسهيل أو القيام في غير الحالات المقررة قانونا بالتقاط أو اختلاس مراسلات تتم أو تنقل أو تصل بطريق الاتصالات و كذلك باستعمال أو فض محتواها. [162]

و يرى جانب من الفقه أن هذه الحماية الجنائية التي يقرها و نص هذه المادة بفقرتيها الأولى و التي ضيقت هذه الحماية الجنائية بإيرادها و باستخدامها بمصطلح "فض" أو بفقرتها الثانية الموسعة لنطاق هذه الحماية.

فإن أحكام هذه المادة تمتد إلى المراسلات الخاصة المتعلقة بمعاملات التجارة الالكترونية عن طريق البريد الالكتروني[163].

كما يرى البعض الآخر أن الحماية الجنائية التي يكلفها للمراسلا ت البريدية و البرقية تمتد إلى

و تمتد الحماية الجنائية التي يكلفها المشرع للمراسلات البريدية و البرقية في نظر البعض إلى سائر صور المراسلات الالكترونية المستحدثة و باستخدام كل الوسائل و الآليات المبتكرة التي يوفرها التقدم العلمي طالما أن هذه الأجهزة و الأنظمة تابعة المشرفة على الاتصالات أو تعهد هذه الأجهزة و الأنظمة تابعة للهيئة المشرفة على الاتصالات أو تعهد هذه الهيئة للغير بأداء خدمات بريدية عن طريقها[164].

و يتوفر الركن المعنوي لهذه الجريمة بالقصد الجنائي العام بعنصريه العلم و الإرادة حيث إذا علم الجاني أنه يخالف القانون إذ قام أو أمر أو سهل فض المراسلات البريدية أو تصنت على وسائل اتصالات و اتجهت إرادته في ذلك إلى إحداث الفعل بنتائجه.

المطلب الثاني : علاقة هذه الجرائم بمعاملات التجارة الالكترونية

---

[161] - حجازي 91، مدحت 105- 106.
[162] - حجازي 92، مدحت 106.
[163] - حجازي 92.
[164] - هشام رستم ، مرجع سابق ، ص 114- 118.

تقوم التجارة الالكترونية على عاملي الإنتاج و الاستهلاك في أغلب معاملاتها و ترتكز العلاقة التعاقدية و آلية نفاذ عمليات التجارة الالكترونية على الإفصاح على بيانات اسمية شخصية إما بالنسبة للمستهل ك أو الطرف الحرفي (الخدماتي) و من شأن الإفصاح عن هذه البيانات أن يرسم أو يعطي تصورا ..... الشخص أو ميولات ه أو اهتماماته و نمط تفكيره الأمر الذي يعد منفذا للإضرار به بصورة مباشرة أو غير مباشرة.

و حتى لو كان شخصا اعتباريا فإن الأمر يزداد تعقيدا حيث التنفيذ في المجالات التجارية قائم على عنصر المنافسة التي قد لا تكون مشروعة إن اعتمدت الإضرار بالغير المنافسين على أساليب جريمة بخصوص التعامل مع البيانات الاسمية، الشخصية للأشخاص الطبيعيين عملائها و كما يمكن إلحاق الضرر بأشخاص اعتباريين كون أن الاسم التجاري أو العلامة التجارية يعتمد على بيانات شخصية و بيانات اسمية و هو ما يمكن أن يشكل خطرا على موقع التجارة الالكترونية و يقدر حماية هذه البيانات الاسمية و الشخصية بقدر ما يكفل لمعاملات التجارة الالكترونية أمان أكثر و تبعث ثقة من شأنها أن تزيد من نمو هذه التجارة الالكترونية و نماءها[165].

ملحق بالجريمة:[166]

بحيث بمجرد الاطلاع عليها يعطي صورة جلية عن الشخص لكن ليس من الناحية المادية فحسب بل حتى من الناحية الشخصية.

و عادة ما يتم حفظ هذه المعلومات من قبل موظفين مؤتمنين بالبريد.

و قد ربط المشرع الفرنسي إمكانية إقامة الدعوى بحصول ضرر لصاحب الشأن و سواء كان هذا الضرر ماديا أو معنويا و إن كان البعض يرى بعدم ضرورة اشتراط حصول الضرر لإقامة الدعوى بل يعاقب الجاني بمجرد مباشرة الركن المادي بمعزل عن حصول الضرر لإخلاله بالتزاماته الوظيفية[167].

---

[165] - **Éric A. CAPRIOLI, Loi du 6 août 2004. Commerce à distance sur l'Internet et protection des données à caractère personnel, Revue Communication Commerce électronique n° 2, Février 2005, Etude 7**

للإطلاع أكثر على علاقة هذه الجريمة بالتجارة الالكترونية، أنظر حجازي 97- 99.

[166] - نعيم مغبغب 195- 197.

[167] **Éric A. CAPRIOLI, Loi du 6 août 2004. Commerce à distance sur l'Internet et protection des données à caractère personnel, Revue Communication Commerce électronique n° 2, Février 2005, Etude 7**

و في معرض الحديث عن عدم احترام الشروط الشكلية فإن الاعتداءات على الحياة الخاصة يمكن أن تطبق بأربع صور:

تخزين و استعمال بيانات شخصية خاطئة.

تخزين أو جمع معلومات بصورة غير قانونية بدون إذن.

إفشاء بيانات بصورة غير شرعية و إساءة استعمالها.

تخطي القواعد المفروضة بتنظيم عملية جمع المعلومات الشخصية و تخزينها و يمكن أن نضيف لها عدم الاحتياط و الإهمال أثناء مباشرة عملية المعالجة (حفظ، تسجيل، نقل...).

صور حيازة البيانات: يمكن أن تحصر في المادة 226- 22:

الحيازة الواقعة بمناسبة تسجيل البيانات

الحيازة الواقعة بمناسبة تصنيف البيانات

الحيازة الواقعة بمناسبة نقل البيانات

الحيازة الواقعة بمناسبة المعالجة العامة[168]

ما هو معيار الضرر المطلوب؟ هل يكتفي بالضرر المادي أم يطال المعنوي؟ [169]

الإفشاء يتمحور حول الاعتداء على الفرد في شرفه أو اعتباره أو حرمه حياته الخاصة[170]

شروط الإفشاء:

يجب أن يتناول الإفشاء إحدى الصفات الواردة آنفا

أن يتم الإفشاء بدون موافقة صاحب الشأن

أن يتم الإفشاء بدون سبب وجيه لتبرير المصلحة العامة[171]

تابع للجريمة:

لا يجب أن تكون المعلوماتية وسيلة للانتقاص من الكرامة الإنسانية أو حقوق الإنسان أو الحياة الخاصة العامة

---

[168] - 199.

[169] - 199.

[170] - 199.

[171] - 200.

تمحورت التشريعات حول الإجراءات الواجبة لإتباع معالجة البيانات الاسمية من جمع و تسجيل و الحفاظ على هذه المعلومات، ووضعت مجموعة أحكام جنائية كوسيلة ردعية ضد أي اعتداء يهدد هذه البيانات أو حرمة الشخص الخاصة بما يوصف أنه إخلال بالشروط الموضوعية و الإجرائية، المنصوص عليها[172]

و قد اهتمت مختلف التشريعات الأوروبية [173]بين جملة من الضمانات القانونية تحمي الأفراد فيها يتعلق بثورة المعلوماتية، و تمديد كيفيات توظيف تلك المعلومات المخزنة أو المتعامل معها يجب أن تكون المعلوماتية في ضجة الأفراد، دون المساس بالهوية الشخصية للأفراد بالحريات الفردية و الجماعية [174]و هو ما أكده القانون 1778 (6 يناير 1978) في الفصل الأول من المادة الأولى.

و حرم ذات القانون أي حكم قضائي أو إداري مادته 02 يكون مؤسسا على معلومات مستمدة من المعلومات الشخصية لتحديد الفرد أو إصدار رأي على الشخص محل الحكم أو المتابعة[175].

و فرضت المادة 03 ضمانات خولت لكل شخص معارضة المعلومات الشخصية المخزنة في حقه أو النتائج المتوصل إليها[176]

يلاحظ على الدساتير العربية[177] أنها تختلف من حيث تنصيصها لحق الخصوصية حيث نصت عليه معظم دساتير الدول لكن تجاهلت صيانة هذا الحق مما يمكن أن تهدده التطورات التقنية في مجال المعلوماتية الحديثة . و إن وجد التنصيص فإنه يرد في إطار عام غير مرفق بنصوص تنفيذية مفسرة و ضابطة للمراكز القانونية [178] فالنص على هذا المبدأ الدستوري (حق الخصوصية) اختصر عند بعض المشرعين في الوسائل التقليدية (مراسلات بريدية، برقية..) غير أن البعض الآخر قد جاء النص فيه

---

[172] - فوزي أوصديق، 49.

[173] - ففي بلجيكا مثلا من قانون خاص بحماية المعلومات ذات الطابع الشخصي بتاريخ 1992/12/08، فوزي أوصديق 63.

[174] - **Agathe LEPAGE, Réflexions de droit pénal sur la loi du 6 août 2004 relative à la protection des personnes à l'égard des traitements de données à caractère personnel, Revue Droit pénal n° 3, Mars 2005, Etude 5**

[175] - فوزي أوصديق 51.

[176] - فوزي أوصديق 52.

[177] - راجع إيراد النصوص الدستوري حول المبدأ الدستوري المتعلق بحق الخصوصية، فوزي أوصديق 53- 55.

[178] - فوزي أوصديق 53.

مواكبا للتصورات التقنية لوسائل الإتصال حيث أورد لفظ أو أي وسائل أخرى مما يعطي القاضي سلطة التفسير الموسع[179].

يلاحظ أن المشرع الفرنسي عندما أعطى حق الاعتراض على أي عملية تحمل صفة التسجيل أو الحفظ أو الجمع بدون إذن مسبق للشخص المعني قد أقام الاعتبار للقيم الإنسانية على حساب التطورات التكنولوجية[180]

مبادئ و شروط المعالجة: أورد البند 30 من التعميم الأوروبي 46/95 الصادر بـــ 1995/10/24 الخاص بحماية الأفراد من جمع المعلومات ذات الطابع الشخصي:

رضاء الشخص المعني (صاحب الشأن)

أن تكون ضرورية لعملية المعالجة

أو احتراما لالتزام قانوني منصوص عليه

أو لاستخدامها في أغراض تجارية، أو نفعية[181]

[179] - فوزي أوصديق 55.

[180] - فوزي أوصديق 56.

[181] - فوزي أوصديق 57.

المبحث الثالث : المسؤولية الجنائية لمقدمي الخدمات الوسيطة الخاصة بالإنترنيت :

ميزة المعاملات التجارية الالكترونية أنها ليست المعاملات التجارية التقليدية حيث تتم بين طرفي المعاملة عادة فقط – دون وسطاء – لكن الأولى تتطلب تدخل العديد من الأشخاص في المعاملة التجارية كوسطاء كي تتم المعاملة التجارية الالكترونية لذلك كان لزاما التطرق لمسؤولية هؤلاء الأشخاص من الناحية الجنائية[182]

و هم على التوالي: متعهد الوصول، متعهد الإيواء، المنتج، ناقل المعلومات، متعهد الخدمات، مورد المعلومات، مؤلف الرسالة[183].

لما يشكل وسيلة التعامل الجديدة من مخاطر وجب تجديد المسؤوليات الجنائية لهؤلاء بالأخص و أن طريقة السداد ابتدعت فيها طرق الكترونية فيما يعرف بالنقود الالكترونية[184].

المطلب الاول : الطبيعة القانونية لمسؤولية وسطاء الخدمة:

الفرع الاول : موقف التوجيه الأوروبي من مسؤولية متعدي الإيواء:

صدر هذا التوجيه في 08 يونيو 2000 و هو يحمل رقم 31/2000 و تضمن دراسة و معالجة الجوانب القانونية للتجارة الالكترونية و قد خصصت القسم الرابع فيها لمسؤولية الوسطاء[185] و أكد أن الاختلاف بين قوانين الدول الأعضاء بشأن مسؤولية مقدمي الخدمات باعتبارهم من الوسطاء يعوق التجارة الداخلية و الخارجية و أوجب على مقدمي هذه الخدمات العمل على وقف الأنشطة غير المشروعة كما دعا الدول الأعضاء إلى اعتماد مجموعة من الوسائل و الأساليب الفعالة لمنح تلك الأنشطة غير المشروعة[186].

كما أكد التوجيه أو أورد إعفاء من المسؤولية للوسطاء الذين يقتصر نشاطهم أثناء نقل البيانات أو تخزينها على الدور السلبي بما يفترض عدم تدخلهم في تعديلها أو إنشائهـــا[187]

بل يتعامل تعاملا فنيا مع المعلومات التي تأتي من الغير[188].

---

[182] - مدحت رمضان عبد الحليم ، مرجع سابق ، ص 119.

[183] - حجازي 133.

[184] - مدحت رمضان عبد الحليم ، مرجع سابق ، ص 119.

[185] - حسين منصور 189.

[186] - حجازي 114، مدحت رمضان عبد الحليم ، مرجع سابق ، ص122.

[187] - أما التدخل حسب ما تقتضيه طبيعة العمل أي التدخل الفني فلا تتبعه مسؤولية فهو لا يعني تعديلا و لا تعاملا مع موضوع المعلومة أو البيانات، مدحت رمضان عبد الحليم ، مرجع سابق ، ص169

[188] - شيماء عبد الغني ، مرجع سابق ، ص عبد الغني 168.

و أشارت المادة 12 من ذات التوجيه أنه يتوجب على الدول الأعضاء عدم مساءلة من يقوم بتوصيل الخدمة إلا إذا كان هو مصدر المعلومة أو قام باختيار أو تعديل البيانات كما أعطى صلاحية التدخل لأي جهة إدارية أو قضائية تبعا للأنظمة الداخلية لكي تطلب من مقدم الخدمة و تطلب منه وقف أية مخالفة قائمة أو أن يبلغ و يخطر بأي مخالفة وقعت[189].

قررت ذات الأحكام في المادة 13 بخصوص من يقوم بالتخزين لنقل المعلومات[190].

كما دعى التوجيه الأوروبي الدول الأعضاء عدم مساءلة متعهد الإيواء عن البيانات و الرسائل المخزنة متى كانت غير مشروعة بشرط ألا يكون متعهد الإيواء عالما بهذه البيانات غير المشروعة، لكن في حالة علمه بذلك وجب عليه اتخاذ كل التدابير و الإجراءات اللازمة ليسحب تلك المعلومات أو البيانات أو يجعل الدخول إلى الموقع غير ممكن الإطلاع عليه [191] مع عدم الإخلال بحق الجهات الإدارية أو القضائية للدول الأعضاء في توجيه وسطاء خدمة الإنترنيت لمنع نقل أي بيانات غير مشروعة أو إخطارها بوجود مثل هذه البيانات[192].

أي أن التوجيه الأوربي ألزم وسطاء الخدمة إخطار السلطات العامة دون تأخير عن أي نشاط غير مشروع يمارسه مستخدمو الخدمة، و في إجراء يمكن أن يعد تقنية لمجال نشاط هؤلاء الوسطاء فقد ألزمهم التوجيه بتقديم المعلومات التي تمكن من معرفة المستفيدين المتعاقدين معهم في المادة 15 منه[193].

أما في فرنسا فقد صدر القانون رقم 719/2000 الصادر في 2000/08/01 مضيفا المادة 8/43 نفت قيام المسؤولية الجنائية و المدنية لأي شخص طبيعي أو معنوي يقوم بمقابل أو بدون مقابل بالتخزين المباشر و الدائم ليضع تحت تصرف متعاملي ن الخدمة إشارات أو كتاباته أو صور أو صوت أو رسائل[194] إلا في حالتين:

إذا تم اللجوء إلى القضاء و لم يقم القائم بالتخزين أو متعهد الإيواء باتخاذ الإجراء أو التدابير اللازم اتخاذها نحو منع وصول هذا المضمون إلى الجمهور

---

[189] - حجازي 115، مدحت رمضان عبد الحليم ، مرجع سابق ، ص123.

[190] - شيماء عبد الغني ، مرجع سابق ، ص عبد الغني 168، حجازي 115، مدحت رمضان عبد الحليم ، مرجع سابق ، ص123.

[191] - شيماء عبد الغني ، مرجع سابق ، ص عبده 169.

[192] - مدحت رمضان عبد الحليم ، مرجع سابق ، ص123، حجازي 115.

[193] - شيماء عبد الغني ، مرجع سابق ، ص عبده 169.

[194] - حجازي 121- 122.

إذا أخطر من قبل الغير بأن البيانات التي يخزنها غير مشروعة و لم يتخذ إجراء ضد ذلك لمنعه[195].

01- رأي مجلس الدولة بالموضوع:

وافقت الجمعية العمومية لمجلس الدولة على التقرير الصادر عن قسم التقارير و الدراسات التابع للمجلس بشأن الإنترنيت و الخطوط الرقمية بتاريخ 02 يوليو 1998 و يعد أهم الأعمال التي تعرضت للمشكلات القانونية الخاصة بالتجارة الالكترونية و الإنترنيت في فرنسا و قد فصل

التقرير موضوع المسؤولية الجنائية لمقدمي الخدمات الوسيطة كونها من المسائل الهامة لتنظيم نشاط هذه التجارة[196].

و بشأن الحلول القانونية المقترحة التي عرضها التقرير نذكر فيها:

- من بين هذه الحلول أنها أعفت مقدم الخدمة الوسيطة من المسؤولية إلا إذا اتضح من حيثيات و ملابسات النشاط عملهم بالمحتوى غير المشروع للمادة المنزلة في الشبكة أو الموقع[197].

- إقامة المسؤولية التابعية أو التلقائية تشمل مقدمي الخدمات الوسيطة لتسهيل و تحريك الدعوى العمومية[198] اعتمادا على الأحكام العامة للمسؤولية الجنائية لإمكانية مساءلة القائم بالأعمال المتعلقة بالإنترنيت بوصفه فاعلا أصليا أو فاعلا مع غيره أو مساهما تبعيا أو شريكا طالما قام متعمدا بوضع المعلومات غير المشروعة تحت تصرف العملاء[199].

و في إطار تحديد مسؤولية الوسطاء في خدمات المعاملات التجارية الالكترونية خاصة و معاملات الإنترنيت عامة، نجد أن المشرع الألماني قد استهدف إخضاع من لهم صلة أو علاقة بالمعاملات الالكترونية و بالأخص معاملات التجارة الالكترونية للقواعد

---

[195] - منصور حسين 190.

[196] - مدحت رمضان عبد الحليم ، مرجع سابق ، ص،124، أنظر أيضا:
Nathalie DREYFUS, De la responsabilité des intermédiaires techniques : contrefaçon ou responsabilité civile ? Revue Communication Commerce électronique n° 1, Janvier 2007, Alerte 1

[197] - حجازي 124.

[198] - مدحت رمضان عبد الحليم ، مرجع سابق ، ص125.

[199] - حجازي 125، مدحت رمضان عبد الحليم ، مرجع سابق ، ص128.

القانونية العامة من الناحية المدنية أو الجنائية أو الإدارية فأصدر قانون 1997/01/01 حدد فيه الأعمال التقنية الوسيطة في مجال الإنترنيت و قرر عدم مسؤولية وساء الخدمة إلا في حالات محددة حصرا و جعل القواعد القانونية العامة عند مساءلتهم[200].

و قام بالتفرقة بين مجموعات المتدخلين في الخدمة فتبعا لمصدر المضمون بين طائفتين مسؤولية مورد المضمون أو مؤلف المعلومة أو البيانات و هؤلاء لا تثور صعوبة بشأنه تحديد مسؤوليتهم و الطائفة الثانية هم الأشخاص الوسطاء الصادر عن غيرهم المضمون فرأى أن مسؤولية كل وسيط تتوقف على طبيعة دور كل منهم و نشاط، حيث رأى البعض أن العبرة عدى تأثير الوسيط في المضمون و رأى آخرون أن العبرة بمدى رقابته للمضمون[201]

كما تضمن قانون التجارة الالكترونية في دونية لوكسمبورغ المسؤولية القانونية لمقدمي الخدمات الوسيطة. فنص في المادة 60 عدم مسؤولية ناقل معلومات قدمها المرسل و عدم مسؤولية من يقدم خدمة الاتصال شريطة أن يكون هو مصدر المعلومة أو اختار المصدر أو اختار أو عدل المعلومات غير المشروعة و نفت المادة 62 المسؤولية عن متعهد الإيواء إذا خزن معلومات[202] لا يعلم بعدم مشروعيتها أو إذا علم بمضمونها فقام بسحبها أو منع الوصول إليها[203].

و كلفت المادة 63 متعهدي الإيواء التزام مراقبة وقوع بعض الجرائم...؟[204]

الفرع الثاني : موقف الفقه من الموضوع/ الإجماع على مبدأ مسؤولية الوسطاء:

يوجد للفقه آراء في الموضوع بخصوص مسؤولية متعهدي الإيواء [205] حيث يحصر البعض دورهم في كونهم وسطاء فنيين بين أصحاب المواقع و بين المتعاملين بالشبكة من المستهلكين و على أساس ذلك لا تقوم أي مسؤولية جنائية في مواجهتهم عن المضمون غير المشروع للمعلومات أو البيانات المتداولة التي يقومون ببثها [206] فليس بالإمكان منطقيا أن يستطيع السيطرة على ملايين الرسائل التي تدخل الشبكة في وقت قياسي[207].

---

[200] - مدحت رمضان عبد الحليم ، مرجع سابق ، ص132.
[201] - حسين منصور 192.
[202] - مدحت 132- 133، حجازي 123.
[203] - حجازي 123، مدحت رمضان عبد الحليم ، مرجع سابق ، ص133.
[204] - مدحت رمضان عبد الحليم ، مرجع سابق ، ص133.
[205] - شيماء عبد الغني ، مرجع سابق ، ص عبده 173.
[206] - شيماء عبد الغني ، مرجع سابق ، ص عبده 173.
[207] - حجازي 123.

و العبرة في نظر البعض هي مدى تأثير الوسيط في المضمون [208]، لكن اتجاها آخر حملهم المسؤولية و أتبعهم إياها كونهم مسئولون عن محتوى البيانات التي يتعاملون معهـــــــا

تسجيلا أو نقلا أو... على أساس أن لديهم الإمكانية و الآلية التي تمكنهم من التحكم و مراقبة تلك البيانات و المعلومات و بالتالي تؤهلهم إلى أن يفرض عليهم التزام التدخل لمنع تداول البيانات و المعلومات و بالتالي محل عدم المشروعية [209] فالوسيط لا يوفر الخدمة فقط بل يملك مراقبتها و التحكم فيها و بذلك يكون مسئولا عن إنتاجها و نشر و توزيع مادة البيانات و المعلومات غير المشروعة [210]،فالعبرة في نظر البعض بمدى رقابة الوسيط على المضمون[211].

بينما ميز البعض بين مختلف الصور التي يمارسها متعهد خدمات الإنترنيت و قد لاحظ جانب من الفقه أن المشرع الفرنسي يقيم مسؤولية الوسطاء في خدمة الإنترنيت بناء على القواعد العامة للقانون الجنائي، و تبعا لانتفاء الركن المعنوي فلا يمكن مساءلة الوسطاء عن أفعال لم تتجه إليها إرادتهم _ كمبدأ عام _ [212]

و لأنه كذلك من شأن القول بافتراض المسؤولية يتعارض مع المبادئ الدستورية و القانونية العامة و خاصة المسؤولية الشخصية و مبدأ المساواة بين المواطنين أمام القانون[213].

ليس هناك من ينكر مبدأ قيام مسؤولية مقدمي أو وسطاء خدمة الإنترنيت و لم يقل أي من الفقهاء بالإعفاء منها لكن الاختلاف واقع من ناحية طبيعة هذه المسؤولية و كذلك نطاق تطبيقها و اجتهدوا في سبيل تحديد مجالها و أسس إعمالها[214].

كما تطال المسؤولية كل من متعهد الوصول و متعهد الإيواء و كل من سهل التعامل بالمضمون غير المشروع بأي وسيلة.

---

[208] - حسين منصور 192.

[209] - شيماء عبد الغني ، مرجع سابق ، ص عبده 173.

[210] - حجازي 123.

[211] **Nathalie DREYFUS, De la responsabilité des intermédiaires techniques : contrefaçon ou responsabilité civile ? Revue Communication Commerce électronique n° 1, Javier 2007, Alerte 1**

[212] - حجازي 124.

[213] - مدحت رمضان

[214] - حسين منصور 191.

و من الصعوبة تحديد هذه المسؤولية و صعوبة تقنيتها بدقة، فلا يمكن الاعتماد على مبدأ البحث عن مسئول تقريبي أو احتمالي بل لابد من إقامة مسئولية على كل شخص على ضوء الدور القائم به و درجة تدخله في تقديم الخدمة، و إذا كانت المعلومات و البيانات المتداولة في شبكة الإنترنيت توظف لإشباع الحاجات المشروعة للمستهلكين و المتعاملين و المتعاملين في إطار العلاقة التجارية الالكترونية فإن جانبا منها _ معتبرا يدعو المشرع إلى الاهتمام بما يمارسه من نشاطات _ يمكن أن يكون محلا لمخالفات و سلوكات غير مشروعة[215] _ و ربما غير مجرمة _ مما قد يكون لها الأثر السلبي على نشاط التجارة الالكترونية بالخصوص و الاقتصاد الوطني على العموم.

الواقع أن ما بين إنتاج البيانات أو المعلومة غير المشروعة و وصولها إلى المستهلك أو المستخدم الطرف الثاني في العلاقة التجارية مراحل عدة تساهم فيها جهود العديد من الأشخاص الذين تتنوع أدوارهم في النشاط الالكتروني (المتعهد، الناقل، الموصل، المورد، المنتج، المؤلف)[216].

ثم إن تحديد المسؤولية الجنائية يعتبر من، أو هو من الدقة بمكان في مجال التحقيق أو التشريع الجنائي خاصة حينما تطرح المسؤولية في صورة أو حول مسألة المضمون المعلوماتي الذي يمكن أن يشكل مساسا بحقوق الغير أو حينما يهدد مراكز قانونية قائمة[217]

فلو أخذنا فرض أن يكون المستخدم مقيم في دولة و مورد الخدمات في دولة ثانية و شركة معالجة البيانات إدخالا و تحميلا في دولة ثالثة فأي القوانين تطبق؟[218]

فهل نضع قواعد عامة لمسؤولية الوسطاء عن أخطاءهم أم نخصص نصوصا لمواجهة كل مخالفة على حده؟[219]

---

[215] - حسين منصور 184.

[216] - **Cyril ROJINSKY, Commerce électronique et responsabilité des acteurs de l'Internet en Europe, Revue Gazette du Palais, 24 juin 2000 n° 176, P. 18**

[217] - حسين منصور 186.

[218] - حسن منصور 186.

[219] - حسين منصور 188.

و لعل الاجتهاد التشريعي الذي سجل تقدما ملحوظا في مجال مسؤولية الوسطاء هو ما أوردته التوجيهات الأوربية المتعلقة ببعض الأوجه القانونية لخدمات شركة المعلومات و بصفة خاصة التجارة الالكترونية[220].

و لعل البعد الجنائي في مسؤولية الوسطاء هو الأسبق في الظهور لما أثير من قضايا[221].

الفرع الثاني : الخدمات الوسيطة في قانون التجارة التونسي:[222]

01 – مسؤولية صاحب المعلومة: أو ما يعرف بمؤلف الرسالة

كلما عدت المعلومة غير مشروعة قامت بذلك مسؤولية جنائية أي إذا احتوى المضمون ما يدخل في نطاق التجريم فمثلا لو تضمنت الرسائل التي ألفها عبارات قذف أو سب فإنه يسأل جنائيا أو إذا تضمنت صورا أو أخبار تشكل تعديا على الحق في الخصوصية أو نشر معلومات تهدد مراكز قانونيا قائما[223] و يعد نشر هذه العبارات بصورة العلاقية (أي على الإنترنيت) هو داع كاف لتوقيع العقوبة الجنائية المقررة بمثل هذه الجرائم حسب القواعد العامة[224].

02– مسؤولية ناقل المعلومات:

دور ناقل المعلومات يتمثل في النقل المادي للمعلومة بوسائل فنية حيث يقوم يربط الشبكات بمقتضى عقد نقل المعلومات بين جهاز المستخدم و بين الحاسبات المرتبطة لمواقع الإنترنيت عن طرق الحاسب الخادم لمتعهد الوصول [225]و عادة ما تتولى هذه المهمة الهيئات العامة للاتصالات بموجب عقد مبرم بينها و بين موردي خدمات الإنترنيت و المشروعات و المنظمات صاحبة الاشتراك على الشبكة كما يمكن أن تستأجر خطوطا متخصصة[226].

و دور الناقل متخصص في تامين نقل المعلومة و الربط بين الوحدات المختلفة و قد عرفت المادة الأولى من القانون الفرنسي رقم 96– 659 سنة 1996 العامل الفني بأنه

---

[220] **Nathalie DREYFUS, De la responsabilité des intermédiaires** techniques : contrefaçon ou responsabilité civile ? Revue Communication Commerce électronique n° 1, Janvier 2007, Alerte 1 انظر ايضا : 189 - حسين منصور

[221] - حسين منصور 189.
[222] - حجازي 129- 132.
[223] - حسين منصور 197.
[224] - حجازي 155.
[225] - حجازي 150.
[226] - حسين منصور 197.

"كل شخص طبيعي أو معنوي يستغل شبكة الاتصالات عن بعد" [227]و المفترض كقاعدة عامة في هؤلاء عدم مراقبتهم للرسائل و المعلومات محل عملية النقل من هذا المنطلق "لا تثور مسئوليته عما يشوبها من أوجه عدم المشروعية بل يلتزم بالحفاظ على سرية المراسلات التي تم عبر الشبكة و الحياد التام تجاه مضمون الرسائل المنقولة"[228].

أما إذا ثبت علم بالطابع غير المشروع للمعلومات التي تعبر شبكة فإن القواعد العامة المسؤولية الجنائية، هي التي تحدد مسؤولية أي متى ثبت له دور إيجابي في نشر المادة المعلوماتية غير المشروعة، و أيضا شريطة توفر القصد الجنائي العام بعنصريه العلم و الإرادة[229].

03- مسؤولية مورد المعلومات:

مورد المعلومة هو شخص طبيعي أو معنوي يتوسط بعمل بين مستخدم الإنترنيت و بين مؤلف مضمونه الموقع فهو يقوم بتحميل الجهاز أو النظام بالمعلومات التي قام بتأليفها أو جمعها حول موضوع معين حيث هو الذي يقوم بالاختيار ثم التجميع و التوريد حتى تصل إلى مستخدمي الشبكة [230] و هو ما يمكن له سيطرة كاملة على هذه المعلومات كونه يملك جمعها و توريدها من عدم ذلك[231].

و قد حاول البعض مشابهته بخدمة وسائل الاتصال المرئية و المسموعة لكن هذا الطرح لم يلقى قبولا [232]كون أن الالتزامات التي ينظمها النظام القانوني لتلك الوسائل لا توفر حرية للتجارة الالكترونية و هذا ما نص عليه التوجيه الأوربي[233].

أما عن مسؤوليته فقد فصل القضاء الاستناد إلى القواعد العامة للمسؤولية بصدد كل المهام خاصة منها القائمة على الوساطة التقنية أو عمليات التجميع و الربط[234] و تتوقف هذه المسؤولية على مدى علم المورد بمضمون المعلومات غير المشروعة و المخالفة للقانون التي يتعامل معها.

أما إذا كان مورد المعلومة هو الذي قام بإنشاء هذه المعلومات محل عدم المشروعية فإن فعله هذا يقع تحت طائلة المساءلة الجنائية (فعلى سبيل المثال إذا قام المورد

---

[227] - حجازي 150.
[228] - حسين منصور 197.
[229] - حجازي 150.
[230] - حسين منصور 199، حجازي 153.
[231] - حجازي 153.
[232] - بل لقي اعتراضا.
[233] - حسين منصور 200.
[234] - حسين منصور 201.

بتصنيع صور مخلة بالآداب العامة فإن المادة 227- 22 من قانون العقوبات الفرنسي تحرم هذا الفعل بعقوبة تسهيل إفساد قاصر).

فمثلا يقع مورد المعلومات تحت طائلة المادة 321- 1 من قانون العقوبات الفرنسي إذا كان حاصلا لمعلومات متحصلة من جنحة _ و إن كان ذلك قد شكل في الأول إشكالا_ و قد تبنى القضاء موقفا أخذ فيه المفهوم إمكانية إخفاء المعلومات المسروقة[235].

04- مسؤولية متعهد الخدمات:

متعهد الخدمات هو مصدر التدفق المعلوماتي و هو المسئول الأول عن المعلومات التي تعبر الشبكة كونه الوحيد صاحب السلطة الحقيقية لمراقبة المعلومات المبثوثة[236] كما أنه ملزم بإخطار النائب العام حسب نص المادة 43 من قانون 1986 بخدمة الاتصال السمعية البصرية، و يلتزم كذلك بأنه يعين شخصا طبيعيا بمنصب مدير للنشر لكي يتحمل المسؤولية الجنائية عن مضمون و محتوى الخدمة (المادة 2/93 من القانون الصادر في 29 يوليو 1982[237].

و لعل أهم التزاماته و هي كثيرة هو مراقبة محتوى الرسائل التي تصل إليه و متى كانت هذه الرسائل مخالفة و الضوابط القانونية قرر عدم نشرها.

و هو يتولى القيام بعدة وظائف و بقدر قدرته الفعلية في السيطرة على المعلومات و التحكم في نشرها و توريدها بقدر المسؤولية الملقاة عليه و هو ما دعى المشرع المصري إلى النص على دور تلك الجهة الوسيطة في قانون التجارة الالكترونية[238] فيما يتعلق خدمات المصادقة على التوقيعات الالكترونية، تشفير المعلومات المتعلقة بالتجارة الالكترونية[239].

05- مسؤولية متعهد الإيواء:Fournisseur d'hébergement

يتولى متعهد الإيواء سواء كان طبيعي ا أو معنويا لتخزين التطبيقات و السجلات المعلوماتية لعملائه، فيعرض إيواء صفحات الويب على حساباته مقابل أجر فهو يؤجر لمكان الشبكة و يمد هؤلاء العملاء بالوسائل التقنية و المعلوماتية التي تسمح لهم في أي

---

[235] - و كان ذلك في سنة 1995 حيث أدانت محكمة النقض الفرنسية إخفاء المعلومات المسروقة تأسيسا على أن حماية المعلومات أمر حتمي في دولة ديمقراطية حتى و لم يكن لهذه المعلومة وجود مادي محسوس، حسام أحمد حسام طه تمام ، مرجع سابق ، ص 252.

[236] - حسين منصور 217.

[237] - حجازي 151.

[238] - حجازي 152.

[239] - حجازي 152/ للإطلاع أكثر على هذه التفاصيل أنظر هدى حامد قشقوش ، مرجع سابق ، ص قشقوس 93- 99.

وقت من الوصول إلى المعلومات المخزنة في النظام، فيملك المتعامل نشر نصوص أو صور أو مناقشة أو روابط تفاعلية أو إنشاء مواقع[240].

و لما كان متعهد الإيواء يسهم في نشر معلومات يتلقاها من مؤلفي من مؤلفي الرسائل عن طريق الوسائل الفنية التي تضعها تحت تصرف مورد المعلومات، هذا النشاط أثار في الفقه جدلا كبيرا و كذا أحكام القضاء[241].

06- مسؤولية متعهد الإيواء:

الاتجاه العام القائم في التشريع المقارن يذهب إلى عدم مساءلة متعهد الإيواء، نجد أن الاتجاه العام للنصوص الواردة تميل إلى إعفاء متعهد الإيواء من المسؤولية عن الفعل غير المشروع الصادر عن الغير و لا يسأل إلا على خطأه هو [242] لأنه ليست له سيطرة على الصفحات التي يتولى تخزينها إلا إذا نشرت أما قبل النشر فلا يسيطر عليها عدا أن تكون الرسالة المجرمة بسجله في وقت سابق و هو ما دعى البعض إلى التفرقة بين فرضين:

الأول: أن يكون متعهد الإيواء شريكا في المخالفة

الثاني: أن يسأل متعهد الإيواء عن جريمة إخفاء أشياء مسروقة[243].

الفرع الثالث : موقف التشريع المقارن:

استبعد النظام الأمريكي المنظم للتعاملات الالكترونية خدمات متعهد الإيواء من المسؤولية عن المضمون غير المشروع للمعلومات المنشورة مادام أن متعهد الإيواء يجهل ذلك و لم يتقاضى مقابلا ماديا جراء المخالفة، و سحب المضمون غير المشروع بمجرد تلقيه إبلاغا عنها[244].

و قد أوجب التوجيه الأوربي الصادر في 8 يوليو 2000 بشأن التجارة الالكترونية على الدول الأعضاء مراعاة عدم مسؤولية مقدم خدمة الإيواء إلا بشروط معينة:

علمه بالمضمون غير المشروع للموقع الذي يؤويه فيسأل جنائيا[245]

---

[240] - حسين منصور 202، حجازي 141.

[241] **Cyril ROJINSKY, Commerce électronique et responsabilité des acteurs de l'Internet en Europe, Revue Gazette du Palais, 24 juin 2000 n° 176, P. 18**

[242] - حسين منصور 202- 203.

[243] - حجازي 141- 142.

[244] - حسين منصور 203.

[245] - حسين منصور 203.

إمكانية غلق الموقع أو منع الوصول إليه أو قدرته على سحب المعلومة غير المشروعة.

01 –متعهد الإيواء كشريك في الجريمة:

الأصل أن لا يسأل متعهد الإيواء حتى يثبت عدم علمه بالمعلومة غير المشروعة حيث بمجرد التعاقد مع مورد الرسالة أو مؤلفها لا يقوم كسبب للمساءلة أو الإدانة و إن كانت غير مشروعة طالما أنه لا يعلم.[246]

و حيث أن الجريمة عمدية فغن متعهد الإيواء لا يسأل جنائيا عن عامل الاشتراك أو الإهمال أو عدم الاحتراز كون الركن المعنوي لهذه الجريمة القصد الجنائي العمدي دون الخطأ أو غير العمدي[247].

يعني عدم وجود المسؤولية عن تحمل التبعة أو المخاطر بل يقوم نتيجة ثبوت الخطأ، فقط يلتزم ببذل العناية لمنع تداول المضمون المخالف للقانون [248] لكن إذا علم متعهد الإيواء بالمخالفة الواردة في المادة المعلوماتية على الحاسب الرئيسي فإن هذه المسؤولية تتوقف على طبيعة الجريمة، فإن كانت الجريمة (مؤقتة) وقتية فعلم متعهد الإيواء بالمخالفة يجب أن يكون مسابقا أو معاصرا لنشر المادة المعلوماتية غير المشروعة و ليس لاحقا لها[249].

أما لو كانت الجريمة مستمرة فإن صفة الاشتراك تتحقق متى انتهى إلى علم متعهد الإيواء بوجود مادة معلوماتية مخالفة للقانون[250].

02 –مسؤولية متعهد الإيواء في جريمة الإخفاء :

يفرق في هذه الجريمة بين حالتين أولها لا تقوم بحقه جريمة الإخفاء إذا اقتصر دور متعهد الإيواء على وضع معلومات غير مشروعة على ذاكرة الحاسب كون أن القضاء لا يعتبر المعلومات كيان مادي يمكن حيازته و به لا يصلح أن يكون محل إخفاء[251].

تراجع المادة 15 من قانون التجارة التونسي فيما يخص موردي خدمات المصادقة.

03 –أثر الجهالة على تحديد المسؤولية:

---

[246] - حجازي 142.
[247] - حجازي 142.
[248] - حسين منصور 204.
[249] - حجازي 143.
[250] - حجازي 143.
[251] - حجازي 143.

عادة ما يلجأ مقدمو الخدمات الوسيطة و فيهم متعهد الإيواء إلى دفع مسؤوليتهم عن مضمون المعلومات غير المشروعة بالاحتجاج بالجهالة أي عدم معرفة مؤلف الرسالة[252].

و يفرق بين الجهالة الظاهرة المتمثلة في رفض متعهد الإيواء الكشف عن شخصية مؤلف الرسالة و بين الجهالة الحقيقية المتمثلة في امتناع متعهد الإيواء عن الحصول عن معلومات شخصية خاصة بمؤلف الرسالة أو عدم التأكد من صحتها إن أمده ببيانات اسمية لكون متعهد الإيواء يفضل إرضاء عملاءه الذين يفضلون عدم الكشف عن بياناتهم و هوياتهم و هو بهذا السلوك و الأسلوب يتهرب من المسؤولية بالدفع بالجهالة[253].

04 –مسؤولية متعهد الوصول:

متعهد الوصول أحد وسطاء الخدمة في معاملات التجارة الالكترونية و هو كل شخص طبيعي أو معنوي ينحصر دوره في تقديم خدمة فنية للعملاء من الجمهور الراغبين في الوصول إلى الإنترنيت، فيزودهم بمقتضى عقد اشتراك بالوسائل الفنية للوصول إلى المواقع التي يرغبونها بتوصيله بمقدمي الخدمات، و ليس علاقة بالمادة المعلوماتية مضمون الرسالة أو مضمون الرسائل المتبادلة على الشبكة[254].

مما دعى البعض إلى وصف دوره بالحيادي فليس له الإطلاع على مضمون المادة المعلوماتية التي تمر عبر الشبكة و لا تعرف عليها، و عليه لا يمكن مساءلته على محتوى هذه البيانات و المعلومات و الرسائل[255].

و تثور بشأن مسؤولية متعهد الوصول كون دوره فني تقني بحت ليس منشئا للمادة المعلوماتية أو مؤلفا للرسالة محل عدم المشروعية مما ينفي عنه المساءلة و لا تقوم إلا إذا قام بخدمة إضافية إلى جانب عمله الأصلي كأن يقترح المادة المعلوماتية فيعد منتجا و بمثابة متعهد معلومات[256].

---

[252] - حسين منصور 207.

[253] - حسين منصور 207.

[254] - حجازي 136، حسين منصور 209.

[255] - **Nathalie DREYFUS, De la responsabilité des intermédiaires techniques : contrefaçon ou responsabilité civile ?** Revue **Communication Commerce électronique n° 1, Janvier 2007, Alerte 1**

[256] - حجازي 136، حسين منصور 211.

بينما رأى فريق آخر مساءلته جنائيا إذا علم بالمادة المعلوماتية محل عدم المشروعية و مضمون الرسالة المخالفة للقانون، و مع علمه لم يتخذ الإجراءات التي يتطلبها القانون من إخطار السلطات المختصة أو سحب المادة، او وقف نشرها أو السيطرة عليها و وقفها.

و إن كان البعض الآخر تشدد أكثر في مساءلته حيث أقام مسؤوليته على أساس المسؤولية المفترضة التي لا يستبعد فيها بعدم علمه فهو يعد موزعا للمادة المعلوماتية حيث هو ينتمي إلى تلك السلسلة التي أقام المشرع نظاما لها يتعلق بكيفية النشر[257] .

و إن كان هذا الرأي الأخير يعد استحالة مطلقة السيطرة على ما يعبر الشبكة من معلومات و قد وصف البعض مساءلته لعدم علمه تأسيسا على المسؤولية المفترضة (التوجيهية) لمساءلة مدير مكتب البريد و الاتصالات اعتبارا على أنه مسئول على تحري مشروعية الخطابات التي توزع و المكالمات التي ترد عن طريق مرفقه[258].

أما فريق آخر فنفى مساءلة متعهد الوصول إطلاقا إذ تمثل دوره فقط في كونه ناقلا فلا يساءل جنائيا عن مراقبة المادة المعلوماتية التي تمر عبر الشبكة _ ما لم يتعهد صراحة بمراقبة المضمون المعلوماتي فهو بذلك يقيم و يشدد مسؤوليته _ أما إذا اختلف دوره كأن يكون متعهد للإيواء أو التخزين أو ناقلا أو مرحلا للمناقشات و المؤتمرات فإن مسؤوليته تتحدد حسب طبيعة الدور الذي يؤديه[259].

أما القضاء فقد عمد إلى إعمال القواعد العامة للمسؤولية الجنائية و عدم إعمال قواعد المسؤولية الجنائية المفترضة في حق متعهد الوصول لان دوره فني ينحصر في توصيل المشترك بالمواقع و ليس له السيطرة على المادة المعلوماتية و لا مراقبة مشروعيتها و هو ما يدعو إلى الرجوع إلى القواعد العامة للمسؤولية متى ثبتت[260].

له دور إيجابي في نشر و بث المعلومة المخالفة للقانون و متى توافر في حقه القصد الجنائي العام _ بعنصريه العلم و الإرادة _ و كان في مقدوره رقابة المادة المعلوماتية

---

[257] - حجازي 137.
[258] - حجازي 137.
[259] - حجازي 137.

[260] **Cyril ROJINSKY, Commerce électronique et responsabilité des acteurs de l'Internet en Europe, Revue Gazette du Palais, 24 juin 2000 n° 176, P. 18**

التي تنقل عن طريقه أو امتنع عن وقف بث المعلومات غير المشروعة مع علمه بطبيعتها الإجرامية.[261]

كما يجب عليه أن يقدم إلى سلطات التحقيق أي بيانات تتعلق بالعملاء متى طلب منه ذلك، و كذلك هو يقوم بالحصول على بيانات تحقيق الشخصية المتعلقة بكل مشترك في بداية التعاقد.[262]

الفرع الرابع : الوضع في فرنسا:

رفع اتحاد الطلبة اليهود في باريس دعوى أمام قاضي الأمور المستعجلة، تمثلت وقائع القضية في كون .... شركات من متعهدي الوصول بمحو ..... بيانات رسائل متعلق موضوعها كتابات عنصرية معادية للسياسة في نظر اتحاد الطلبة اليهود مطالبين القاضي إصدار أمر بإلزام المدعي عليهم منع وصول المشتركين إلى تلك الرسائل أيا كان موقعها في الإنترنيت كون المادة المعلوماتية تمثل مخالفة للمادة 24 مكرر من قانون 12 يوليو 1981 في شأن الصحافة[263].

كما التمس الاتحاد المذكور من القاضي ندب خبير من البحث الجنائي تكون مهمته تحديد ما إن وجدت إمكانية فنية لمنع الدخول إلى الحاسبات الخادمة حيث توجد المادة المعلوماتية محل الدعوى[264].

قابلت المحكمة هذا الطلب كون أن يتسم بالعمومية و عدم التحديد خاصة و أن ما يطلبه اتحاد اليهود أمر مستحيل من الناحية الفنية حيث لا يمكن مراقبة ملايين الرسائل التي تمر بالمواقع[265] بالإضافة إلى أنه قد تكون المادة محل الدعوى مشروعة حسب قانون البلد الصادرة منه .

و دور الوسطاء و إن كان الفقه يؤكد مع القضاء على ضرورة مساءلتهم جنائيا في إطار قيامهم بالخدمة الوسيطة[266].

إلا أن ذلك الدور المتعلق بتوصيل العملاء بالحاسبات الخادمة أي انهم ناقلين أو وسطاء بالنسبة للمعلومات التي تعبر الشبكة فليس من المستطاع مساءلتهم عن مضمون المادة المعلوماتية التي تعبر الشبكة[267].

---

[261] - حجازي 139.
[262] - حسين منصور 212.
[263] - حسين منصور 212.
[264] - حجازي 120.
[265] - حسين منصور 213.
[266] - حسام أحمد حسام طه تمام ، مرجع سابق ، ص 237.
[267] - حجازي 120.

كما نبهت المحكمة بضرورة إلزام المشتركين بضرورة احترام أحكام القانون السابق ذكره و لم .... وسطاء الخدمة.

المبحث الرابع : جريمـــة التهـــرب الضريبـــي

نعلم أن الآليات المعتمدة في النشاط التجاري الالكتروني هي آليات أضافت على هذا النشاط صبغة العالمية أي اختزاله لعاملي الزمان و المكان حيث وفرت هذه الآلية ما كان يشكل فيما سبق عبئا على أطراف العلامة التعاقدية بذات الوقت ربما قد تكون هذه الآلية العابرة للحدود قد خلقت مشاكل جمة للجهات المسئولة عن ضبط تعاملات هذه الآلية من هذه المشاكل المطروحة مشكلات متعلقة بالضرائب[268].

فالمعمول به عند الدول هو خضوع النشاط التجاري لنظام ضريبي، متى كانت رؤوس الأموال السلع و الخدمات يتم تداولها بطريقة مادية تمكن من حصر النشاط التجاري و تحديد الأرباح و تحديد الوعاء الذي يخضع للضريبة المعمول بها حسب التشريع السائد، و من المقر عند البعض [269] خضوع شبكة الانترنيت للضريبة، حيث تطبق القواعد العامة للضريبة على معاملات التجارة الالكترونية فشأنها في ذلك شأن التجارة التقليدية ذلك أن معاملاتها الالكترونية سواء تعلقت بالأموال أو الخدمات تندرج تحت سلطات ضريبة المبيعات، لكن الأمر ليس بذات البساطة بالنسبة للتجارة الالكترونية ذلك أن صعوبات قانونية و إجرائية ستواجه المشرع، فتحديد حجم نشاط التجارة الالكترونية الخاضع للضريبة من إشكالات.

---

[268] **Hubert BITAN , Le site de commerce électronique : approche technique et juridique, Revue Gazette du Palais, 18 avril 2000 n° 109, P. 17**

[269] - محمد حسين منصور، ص 163.

مما نستدعي تعديل القوانين المتعلقة بالتشريعات الضريبة و تشريعات الجمارك لتشمل الضريبة معاملات هذه التجارة[270]

بالإضافة إلى أن المعاملات التي تتم عبر الانترنيت تمتد لتشمل أكثر من دولة مما يشير التساؤل حول تحديد الدولة صاحبة الحق في فرض الضريبة، فمن غير الممكن لأي إطار معاملات التجارة الالكترونية ربط المعاملة بمنطقة جغرافية معينة، مثلما أن عرض الخدمة على الانترنيت لا يسمح للبائعين عبر الشبكة معرفة مكان استخدام خدماتهم و منتجاتهم.[271]

و لذلك فإن جريمة التهرب الضريبي في معاملات التجارة الالكترونية تظهر في حالة وجود تشريعات تنظم كيفات التحصيل و تحديد الوعاء الخاضع لهذه الضريبة، و لما لم يكن هناك اتفاق حول هذا الموضوع و لا تزال آليات المعاملات التجارية الالكترونية تتنامى من حيث الإيرادات و الأرباح لا تزال النظم القانونية غير مسايرة لهذا التطور و التفاعل[272]، و لذلك اقترح البعض ضرورة التفرقة في نطاق معاملات التجارة الالكترونية بين نوعين من المنتجات و السلع و الخدمات:[273]

النـــوع الأول: هو تلك المنتجات أو السلع و الخدمات التي يتم التعاقد عليها الكترونيا و سداد ثمنها كذلك لكن توريدها و استلامها يتم بالطرق التقليدية و هذا النوع يمكن إخضاعه للتحصيل الضريبي وفقا للقواعد العامة التقليدية للضرائب حيث لا يعدو عن

---

[270] - حجازي، ص 324.

[271] - حسين منصور، ص 164.
إذا اتفق طرفي المعاملة التجارية على إخفاء معاملاتها عن مصلحة الضرائب، فلن تتمكن مصلحة الضرائب من تحديد حجم تعاملات الممول التي يحسب على أساسها قيمة الضريبة المستحقة على هذه التعاملات، حجازي، ص 325.

[272] **Michel AUJEAN, L'évolution de la fiscalité en Europe sous l'impulsion de la Commission : 50 ans du Traité de Rome, Revue Gazette du Palais, Communautés européennes, 10 juillet 2007 n° 191, P. 16**

[273] - هدى حامد قشقوش الحماية الجنائية، ص 52.

كونه سلعة أو منتجا كباقي المنتجات فيخضع بذلك لقوانين و تشريعات الضرائب و الجمارك.[274]

النـــوع الثـــاني: و هو ذلك النوع الذي تتم فيه كل المعاملة التجارية الكترونيا من مرحلة العرض و التفاوض إلى مرحلة تسليم السلعة أو الخدمة هذه الطريقة يبنى عليها إشكالا حول كيفية تحصل الضريبة عليها حيث تظهر عند التعامل معها عدة إشكالات أخرى متعلقة بمسألة[275] الازدواج الضريبي: فالقول بفرض ضريبة عليها حتما سيجعل من السلع و الخدمات ذات النشاط..... لأكثر من دولة يعرضها لفرض ضرائب متعددة و هو أمر غير مستساغ.

المطلب الأول :مشـــكلات فـــرض الضريبـــة عـــلى معامـــلات التجـــارة الالكترونيـــة:

تمثل الإنترنيت آلية ارتكاز للتجارة الالكترونية ترتبط بها وجودا و عدما، فهي الوسيط العالمي الذي يمكن من خلاله إبرام الصفقات التجارية و إمضاء العقود الربحية و بذلك فإن هذا الإجراء أو الآلية الالكترونية تشكل تحديا لتلك القيود التي نضمتها آليات التجارة التقليدية، فلقد أصبح من السهل جدا انتهاك تلك الأطر و الضوابط و القيود[276].

فإذا كان من السهل فرض ضرائب على مختلف المبيعات في عالم التجارة التقليدية سواء كان من السهل فرض ضرائب على مختلف المبيعات في عالم التجارة التقليدية سواء أكانت هذه الضرائب على المعاملات التجارية المحلية أو على تلك المعاملات التي تتعدى الحدود الإقليمية للدولة، فإنه بمقدار ذات السهولة تجاهل هذا التنظيم أي أنه

---

[274] - جلال الشافعي، ص 75- 76.
[275] - حجازي، ص 325 / هدى حامد، ص 52.

[276] **Bruno P. LANGLOIS, La protection des marques sur internet : le législateur fédéral américain s'attaque à la cyberpiraterie, Revue Gazette du Palais, 20 juillet 2000 n° 202, P. 29**

من السهولة جدا التهرب من الأطر و الضوابط التي تنظم الطريقة و بشكل كلي أحيانا.[277]

إلا أن لغياب تلك الأطر المنظمة و القواعد الضابطة للضريبة و إنها بشكل أبسط أن نطاق التجارة الالكترونية غامض و غير مستقر و ربما يكون مرجع ذلك غير ملموسة و بغياب الكيان المادي لمراكز التجارة الالكترونية يصعب و لا يستحيل إيجاد قواعد ضريبية على الأقل للوقت الحالي، فعندما تتنوع الضرائب على التجارة الالكترونية، فإن التأكد مما هو خاضع للضريبة و من المسئول عن دفعها يكون أمرا معقدا لما يمكن أن يسببه فرض ضرائب على التجارة الالكترونية كخدمة اتصالات، أو خدمة معلومات أو غيرها من تداخل و خلط في قانون الضرائب و يوقع في إشكالات الازدواج الضريبي.[278]

الفرع الأول : الصعوبات العملية

و هي متعلقة بمسألتين أولها هي، عدم قدرة مصلحة الضرائب على تحديد قيمة و مقدار الوعاء الخاضع لهذه الضريبة و ما يبنى على ذلك من تحديد مقدار الضريبة على وجه الدقة لما بإمكان أطراف العلاقة التعاقدية من قدرة على إخفاء حقيقة تعاملاتهم عن المصالح الضريبية[279].

هذه الصعوبات جعلت من جريمة التهرب الضريبي جد ممكنة و سهلة و محاولة إقرار حماية جنائية تجاهها أمر غير مطروح آنيا لعدم ثبات الأطر الضابطة للضريبة أصلا و لذلك وجدت العديد من المقترحات لإلغاء هذه الضريبة و إعفاء المعاملات التجارة الاكترونية من كل الرسوم الضريبية و الجمركية. كما جاء في الإعلان

---

[277] - عماد حداد، اللجنة العلمية للتأليف و التحرير و النشر، التجارة الالكترونية، سلسلة كويك نوتس، دار الفاروق، ص 55.

[278] - طارق عبد العال حماد، التجارة الالكترونية المفاهيم التجارب التحديات الأبعاد التكنولوجية و المالية و التسويقية و القانونية، الدار الجامعية، الإسكندرية، ص 679- 680.

[279] **Hubert BITAN , Le site de commerce électronique : approche technique et juridique, Revue Gazette du Palais, 18 avril 2000 n° 109, P. 17**

الوزاري في ماي 1997 لمجموع 132 دولة حيث أوحى بعدم فرض هذه الضريبة على نشأة التجارة الالكترونية.[280]

و إن كان من شأن هذا المقترح أن..... إلى عدم مساواة في إطار المعاملة الضريبية للنشاط التجاري على وجه العموم بالإضافة إلى أن أي نظام قانوني في أي دولة يكفل حماية قانونية (مدنية أو جنائية) لممارسة التجارة الالكترونية، ما يدعوا لأن تحصل الدولة على تكلفة المزايا التي تضمنتها لأطرف هذه التجارة.

هذه المزايا يمكن أن تحصلها الدولة في شكل رسوم و ضرائب، كما يرى البعض.[281]

و من أهم الصعوبات التي تثيرها معاملات التجارة الالكترونية أمام أجهزة فرض الضرائب جبايتها ما يلي:[282]

- سهولة التهرب من دفع الضرائب غير المباشرة مثل ضريبة المبيعات و ضريبة القيمة المضافة، الرسوم الجمركية فيما يتعلق بالسلع القابلة للنقل الالكتروني (الافتراضية)
- كون دفع الضرائب بالحدود الجغرافية للدولة فالطابع العلمي للمعاملة التجارية الالكترونية يحول دون تنظيم محكم للضريبة آنيا.
- صعوبة التعرف على هوية الأفراد و الشركات و المتعاملين آلية الإنترنيت، و كذا مكان تواجدهم أضف إلى ذلك أن تطور أسلوب الدفع الالكتروني لا يمكن للسلطات من تتبع آثاره فوسائل التحقق من الشخصية التي تتعامل مع الانترنيت تعد ذات طبيعة احتمالية مما يعني استحالة مراقبة المعاملة الالكترونية، فالطلبات و الفواتير عرضة للتزييف و هو ما يخلق إشكالا حول كيفية تتبع المعاملات و عمليات التسليم و أداء الخدمات و الوفاء مع الجهات المصرفية.[283]

---

[280] - هدى حامد ح ج ، ص 53.

[281] - حجازي، ص 326.

[282] - إبراهيم العيسوي، التجارة الالكترونية ، المكتبة الأكاديمية، 2003، مصر، ص 109.

[283] - محمود حسين منصور، المسؤولية الالكترونية، ص 166.
فتحديد الموقف الضريبي للممول، و تقدير الضريبة و تحصيلها يتطلب أن تطلع الإدارة الضريبية على البيانات الضرورية التي تلاءم تطبيق الضرائب على الدخل أو على المبيعات أو غيرهما و أهم هذه البيانات: إسم الممول أو المكلف، عنوان منشأته، محل إقامته، كيانه القانوني، بيانات أساسية عن الصفقات و المعاملات التي أبرمها،و بيانات عن المتعاملين، جلال الشافعي، ص 85.

ممن يصعب تحديد من يخضع للضريبة و كيفية إلزامه بدفعها:

- توسع نطاق الخيارات لدى المتعاملين بالتجارة الالكترونية من أفراد و شركات فيما يخص الانتقال من بلد لآخر، حسب انخفاض معدلات الضريبة أو تركيز النشاط في بلاد معفي التعاملات الالكترونية من الضرائب.
- صعوبة حصر التعاملات و التعاقدات الالكترونية، برغم من إعمال وسائل الحصر و الإثبات إلا أنها تصطدم بتلك الحقوق الدستورية المتعلقة بالحق بالخصوصية أو انتهاكها من خلال تتبع تدفق البيانات عبر الإنترنيت.
- عدم مرور بعض المنتجات التي يتم شراءها عن طريق الإنترنيت على نقاط جمركية مما يعني عدم خضوعها للضريبة، بينما قد تسلم بضائع أو منتجات أو سلع في شكل مادي مألوف (بريد عادي، رسائل نقل أخرى...) مع العلم أن آلية البيع تمت الكترونيا لكن مرورها على نقاط جمركية يعني خضوعها للضريبة و هذا بحد ذاته يشكل ازدواجا في معاملة منتجات المعاملة التجارية الالكترونية و عدم مساواة بين متعاملي التجارة الالكترونية.
- عدم وجود تنسيق بين المصالح الضريبية و بين وسطاء العمليات التجارية الالكترونية (مزود خدمات، بنك...) حيث هؤلاء بإمكانهم الإسهام في جباية الضرائب بشكل فعلي و بذلك تفقد الإدارة الضريبة مصدرا هاما من مصادر الحصول على بيانات الممولين و تعاملاتهم.[284]

المطلب الثاني : طـــرق مقترحـــة

تم اقتراح بعض الأساليب للتغلب على تلك الإشكالات منها:[285]

الفرع الأول : أسلـــوب الحيـــاد الضريبـــي الالكترونـــي

تزعم هذا الاتجاه الولايات المتحدة الأمريكية حيث نادوا بإلغاء كافة أنواع الضرائب و الرسوم المفروضة أو التي تفرض على السلع و الخدمات و الصفقات التي تتم عبر

[284] - جلال الشافعي، ص 87.
[285] - حسين منصور، ص 166- 169.

شبكة الانترنيت[286] أي بواسطة آلية التجارة الالكترونية رغبة في تحرير هذه التجارة من جميع المعوقات و القيود التي قد تحد من انتشارها و تعاظمها،[287] و جعل الانترنيت منطقة تبادل حر مستبعد من نطاق الضرائب، و لإقرار مساواة بين المتعاملين التجاريين في مجال التجارة الالكترونية، اقترح أن تخضع الضريبة الالكترونية لمبدأ الحياد الضريبي أي أن تتم المعاملة الضريبية بنفس الأسلوب على كل صور التجارة دون تميز.[288]

الفرع الثاني :خلــق ضرائــب الكترونيــة جديــدة:

رأى أصحاب هذا الاتجاه ضرورة تفعيل التنسيق و التعاون الدوي و كخطوة عملية لذلك اقترح أن يعقد مؤتمر دولي يحدد كيفية الحصول على الضريبة و يحدد القائمين عليها كما اقترح أن تجنى الضريبة من طرف الدول المستقبلة للسلعة أو الخدمة.[289]

لكن لم يكن من شأن هذا المقترح أن يكون عمليا و فعالا و ذلك أن من السلع و الخدمات و المنتجات ما لا تمر عبر المنافذ الجمركية أو حتى تعلم بها الدول المستقبلة لها لخروجها عن نطاق السيطرة و الرقابة و الحصر.

و رأو أنه إذا كان تداول سلع و خدمات و صفقات التجارة الالكترونية بالوسائل و الطرق العادية فليس هناك داع لتشريع ضريبي لكفاية التشريع العادي.

بينما إذا كانت السلع المطروحة للتداول تورد من صاحب نشاط إلى صاحب نشاط آخر من خلال التجارة الالكترونية فإن الضرائب المستحقة على هذه السلع تحصل باستخدام

---

[286] - قرر الكونجرس الأمريكي سنة 1998 وقف فرض ضرائب جديدة على التجارة الالكترونية لمدة 3 سنوات و مدد لسنتين أخرتين عام 201 و درس الكونجرس إمكانية جعل منع فرض الضريبة على الإنترنيت و دائما و هذا راجع للإخفاق الذي حققه تقرير اللجنة الاستشارية الخاصة بالتجارة الالكترونية عام 2000 المشكلة بقانون إلغاء الضرائب على المعاملات و الصفقات التجارية التي سيتم إبرامها عبر الانترنيت لعام 1998، في عرض أية إرشادات أو نصائح واقعية فيما يتعلق بالكيفية التي يجب اتباعها قصد تشريع خاص بالضرائب على الانترنيت، عماد الحداد، كويك نوتس، ص 56.

[287] - جلال الشافعي، التجارة الالكترونية و الضرائب، مجلة البحوث التجارية الزقازيق، العدد 02، 2002، ص 75 / المجلد، ص 24.

[288] - حسين منصور، ص 167.

[289] - حسين منصور، ص 167.

آلية التكليف العكسي أي أن يلتزم المستفيد بسداد الضرائب للإدارة الضريبية بدلا ممن قام بالتوريد.[290]

و هذا طرح غير منطقي كما أنه نظري غير قابل ستطبق بل أنه..... عليه بحكم عدم إمكانية و استحالة إحصاء المستفيدين من الخدمات التي تتم الكترونيا.

الفرع الثالث : أسلـــوب الغيـــر محـــل الثقـــة الضريبيـــة

لا تخلو المعاملة التجارية الالكترونية من وجود وسيط بين طرفي العلاقة التعاقدية، و لذلك اقترح البعض اللجوء إلى الغير محل الثقة الضريبية فمثلا في مورد خدمة الانترنيت، البنك، و تقديم نطاقات الائتمان، متعهد الاتصالات، و تكون مهمته في تحديد أطرف العلاقة التعاقدية التجارية التجارية، و تخزين المعلومات المتعلقة بتلك المعاملات و نقلها إلى مصلحة الضرائب.[291]

لتفعيل هذا المقترح اقترح نظام الوسيط المالي لكي يحصل الضريبية عن المعاملات التجارية حيث أن يتولى بنفسه تطبيق الضريبة المفروضة على المتعاملين، و لعل هذه الفكرة هي أكثر واقعية و عملية حيث أن نظام الفحص الالكتروني الذي يربط صاحب البطاقة و البائع بالبنك نظام أكثر واقعية و عملية حيث أن نظام الفحص الالكتروني الذي يربط صاحب البطاقة و البائع بالبنك نظام أكثر أمان و يصعب اختراقه و لذلك يعد نظام تحصيل الضريبة عن طريق الوسطاء الماليين أقرب هذه الآراء للعمل به.[292]

- تطوير التشريعات الضريبية لأجل صياغة نموذج ضريبي للدول يمكنها من تحديد سيادتها على الدخل المحقق من صفقات المعاملات التجارية الالكترونية.
- إحداث تعديلات على الاتفاقيات الضريبية قصد الحد من الازدواج الضريبي مع إعداد مشاريع اتفاقيات جديدة تسمح بتبادل المعلومات على نطاق واسع.

---

[290] - جلال الشافعي، ص 76.

[291] - حسين منصور، ص 168.

[292] - لأجل تحقيق نتائج هذا المقترح ينبغي على السلطات الضريبية أن تحت مورد نظم الدفع الالكتروني على استخدام تلك النظم بالأسلوب الذي يسمح بالإجراء المحاسبي الذي يتفق و تدفق الأموال متبعا للتشريعات السارية على أنه لا يمس ذلك بالأسرار المهنية أو التجارية و لا بالحق في الخصوصية، أنظر حسين منصور، ص 168 / جلال شافعي، ص 87.

- تحسين الخدمات الضريبية بالاستفادة من التطورات التكنولوجية بحيث توفير آليات لدى هذه المصالح لتبادل المعلومات الكترونيا بين المصلحة الضريبية و بين الممولين لخفض التكاليف و ربح الوقت، و يمكن المتعاملين من فهم المعاملات الضريبية و طريقة حسابها و المعلومات و التي يتعين تزويد المصالح الضريبية بها، مما يعمل على مكافحة التهرب من الضرائب الصرامة في اتخاذ التدابير مخالفة قوانين الضرائب، بالمتابعة القضائية و المساءلة لتحصيل مستحقات الضرائب و سداد الغرامات.
- البحث و العمل على إيجاد أدلة إثبات عصرية قابلة للمراجعة و التحقق و ذلك بوضع ضوابط و قواعد قانونية مناسبة لمعاملات التجارة الالكترونية.
- إلزام البنوك و المؤسسات المالية و وسطاء الخدمة بضرورة التعاون مع المصالح الضريبية بإخطار الأخيرة بالتحويلات المالية التي تتم عن طريقها المشروعات.
- إلزام البنوك و الوسطاء في الخدمة (مورد خدمات، مزود خدمات...) بأن تحجر نسبة معينة من هذه التحويلات تحت حسابات الضريبية المستحقة، و تزويدها إلى مصلحة الضرائب المختصة خلال وقت معين من تاريخ، التحويل، فهذه المؤسسات تتم عن طريقها التحويلات المالية بين المشروعات (داخلية و خارجية) من شأن هذا الاقتطاع أن يعتمد كأسلوب ليمنع التهرب الضريبي.
- متابعة التحويلات المالية الالكترونية التي تتم بين المشروعات الأجنبية بواسطة الاطلاع على المستندات المؤيدة لذلك لدى المؤسسات الماليـة و البنكية التي تتم عن طريقها إجراءات التحويلات ثم مطابقة هذه البيانات بالإخطارات الواردة ذات الجهة و بما ورد بالإقرارات المقدمة من الممولين و المكلفين بالضرائب.

الفصل الثاني

جرائم الاعتداء

على مضمون

النشاط

المبحث الأول : جرائم الأموال في نطاق التجارة الالكترونية

وفقا لقواعد العامة في جرائم الأموال:

.....هو من الموضوعات التي نالت اهتماما كبير في القانون الجنائي أيا كان الصفة التي عليها هذا الحق يعاقب على أي من الجرائم التي علن تصور وقوعها على هذا الحق.

و هذه الجرائم بدورها التي تقع على الملكية منصرفة إلى طائفتين:

تضم إحداهما جرائم غايتها إتلاف مال الغير

أما الثانية فالغاية منها الاستيلاء على مال الغير و يدخل ضمن هذه الطائفة جرائم السرقة، النصب، خيانة الأمانة[293].

و عن علاقة هذه الجرائم بموضوع الحماية الجنائية للتجارة الالكترونية نجد أنه يندرج أو منطوي في الإجابة عن الإشكال مفاده:

ما مدى إمكانية وقوع جرائم الأموال على نشاط التجارة الالكترونية ؟

أو هل يمكن تصور وقوع اعتمادات بالجرائم السابقة على نشاط التجارة الالكترونية ؟

لعل الإجابة عن هذا الإشكال قد تتأخر أو تتطلب إجابة عن إشكال ثاني يستدعيه الإشكال الأول و هوى مدى صلاحية المال المتداول في التجارة الالكترونية لأن يكون مالا محميا بنصوص قانون العقوبات، كما يقضي بيانه طبيعة المال المتداول في التجارة الالكترونية.

أكثر الأسواق انفتاحا الآن هو سوق التجارة الالكترونية ذاك أن شبكة الإنترنيت نظام مفتوح للبيع و الشراء سواء للتاجر أو البائع أو المشتري أو الوسطاء بينهما (الحرفي، المستهلك، الوسيط) آليتهم ذلك جهاز الحاسب الآلي و شبكة الإنترنيت أو البطاقات يعترضها العديد من الإشكالات، أهمها ما يمكن أن يتعرض له العميل حين تعرض المعلومات السرية الخاصة برقم الكارت (الكود السري) ثم استخدام هذه المعلومات من طرف آخر للإستلاء على أموال لا يمتلكها[294].

لذاك وجب البحث في أبعاد الحماية الجنائية التي تقررها القواعد العامة في قانون العقوبات في السرقة و النصب و خيانة الأمانة.

---

[293] - حجازي 161.

[294] - حجازي 164.

و يستدعي الحديث عن أبعاد هذه الحماية البحث في مدى إمكانية انطباق وصف المال على المعلوماتية، فلكي تكون هذه البرامج حلا لجرائم الأموال (السرقة، النصب و خيانة الأمانة) لا بد أن يصدق عليها وصف المال أولا و أن تنطوي تحت نصوص التجريم ثانيا.[295]

المطلب الأول : مدى اعتبار المعلوماتية موضوع لجرائم الأموال:

.....

الفرع الأول : صعوبة الحكم جريان جرائم الأموال على التجارة الالكترونية

التجارة الالكترونية نظام قائم على تقنية المعلوماتية، و التشريعات المقاربة تقرران جرائم الأموال تقع على مال لكي يصبح محلا للملكية، و المال هو كل شيء يصلح محلا للحيازة و الأشياء التي تخرج عن دائرة التعامل لا يستطيع أحد أن يستأثر بها[296]، و هذا الأمر لا يثير أي صعوبة في إعمال هذا المفهوم بالنسبة للأموال المنقولة التقليدية، غير أن الإشكال يطرح إذا تعلق الأمر بمفهوم المنقول المعلوماتي بسبب الطبيعة الخاصة لهذا المنقول [297] إذ الجريمة في نطاق المعلوماتية لها ذاتية خاصة فقد يقع الاعتداء على الكيان المنطقي كما قد يحدث على أداة المعلوماتية المادية (دعامة ممغنطة، أقراص...) فلا تثار في ذلك صعوبة قانونية ذلك أن الدعامة تعتبر مالا منقولا تحميه نصوص التجريم في جرائم الأموال فهذا الاعتداء مادي فهل يمكن الاعتداء بسرقة البيانات اللاسلكية أو المعلومات ذات الطبيعة المعنوية، و التي يمكن بالطرق الفنية سرقتها بما يعرض صاحبها سواء كان شخص أو شركة لأضرار مادية أو أدبية؟[298]

فعلى خلاف المعلومة تكتسب الدعامة طابعا ماديا محسوسا يؤكد أنه في الفرض الذي يكون فيه للمال طبيعة معنوية و ليس مسجلا على دعامة مادية فإن صعوبة قانونية تثار حول حمايتها بالتجريم الوارد في جرائم الأموال.

و قد كان منحنى التشريعات المقارنة و أحكام القضاء تذهب إلى عدم وقوع جرائم الأموال على هذه الكيانات (المعلومات ذات الطبيعة المعنوية)، لكن معالجة القضاء لهذا الموضوع أخذ تطرأ عليها شيء من التغيير، و منذ وقت ليس بالبعيد اطردت أحكام

---

[295] - علي عبد القادر القهوجي ، مرجع سابق ، ص 80.
[296] - حسام أحمد حسام طه تمام ، مرجع سابق ، ص 453.
[297] - شيماء عبد الغني ، مرجع سابق ، ص عبده محمد 30.
[298] - حسام أحمد حسام طه تمام ، مرجع سابق ، ص 451.

القضاء في أوربا القول بوقوع السرقة على المعلومات كما في بلجيكا مثلا [299]، و أصبح بعض المشرعين يقدرون أن المعلومات تصلح أن يرد عليها النص الخاص بالسرقة استنادا على كونها أصبحت محلا للتجارة الالكترونية [300] و كذلك الفقه فقد بدأ اتجاه بدأ يعتد بصفة المنقول لهذه المعلومات الالكترونية حيث يرون أن المعلومات أموال يصلح أن يرد عليها النص الخاص بالسرقة على نفس السند الذي أسس عليه القضاء رأيه و هو أنها أصبحت محلا للتجارة.

الفرع الثاني : ظهور فكرة المنقول المعلوماتي في جرائم الأموال

خرجت الطبيعة المعنوية للمعلومات الإلكترونية تحديا أمام المشرع و ذلك لما ترتب عن عدم تجريم الاعتداءات الواقعة على هذه الكيانات و التي نتج عنها ضرر جعل القانون الجنائي أمام أزمة حقيقية في مواجهة واقع اقتصاد المعرفة و التقنية أو ما يسمى بالاقتصاد الرقمي أو الافتراضي، فالقاضي الجزائي مقيد عند نظره في الدعوى الجنائية و بمبدأ شرعية الجرائم فلا يستطيع أن يجرم ما لم تجرمه النصوص و لم يجرمه المشرع و لو كانت أفعالا مستهجنة و على قدر متقدم من الخطورة الإجرامية[301].

و لم تكن نصوص قانون العقوبات تتضمن أيا من النصوص الخاصة لحماية التجارة الالكترونية و بالأخص في مجال صناعة و استغلال الحاسبات الآلية، و لعله من غير المجدي البحث عن تلك الحماية من خلال الجرائم التقليدية المنصوص عنها في قانون العقوبات (فضلا عن عدم تجريمها إطلاقا) و الاستثمار في مجال المعلوماتية أصبحت له صناعة و تقنية و تخصيص و ربما هو مفروض و ليس أمام خيارات و المعلوماتية أصبح لها بسوق و هو ذو مصدر للثروة [302] و هو ما يستدعي توفير حماية جنائية لهذه التجارة و الملاحظ أن المشرع لم يكن في تصوره وقت وضع قانون العقوبات.

و الذي يستدعينا لطرح هذه الفكرة هو تساءل البعض عم مدى إمكانية استجابة القاضي الوطني بقانون العقوبات التقليدي لتوفير الحماية لهذه القيمة الاقتصادية الحديثة أي أموال التجارة الالكترونية في ظل النصوص التقليدية خاصة [303] و أن المشرع لم يكن في تصوره وقت وضع تلك النصوص التقليدية مثل هذا التطور في التقنية و هو مكمن

---

[299] - شيماء عبد الغني ، مرجع سابق ، ص عبده 32- 33.
[300] - شيماء عبد الغني ، مرجع سابق ، ص عبده، 34.
[301] - آمال قارة ،مرجع سابق ، ص 13.
[302] - علي عبد القادر القهوجي ، مرجع سابق ، ص 79.
[303] - آمال قارة ،مرجع سابق ، ص 13.

الخطورة في التعامل حيث القانون الجنائي له مبادئه و أصوله و أهمها مبدأ المشروعية و الذي يتفرع عنه مبدأ التفسير الضيق و حظي القياس في مجال التجريم[304].

فهل يمكن للقاضي الجزائي من خلال النصوص الحالية لجرائم الأموال أن تحقق حماية جنائية لمعاملات التجارة الالكترونية و دون المساس بالمبادئ الراسخة التي يرتكز عليها القانون الجنائي[305].

و على الرغم من الطبيعة المعنوية للمعلومات المتعلقة بالتجارة الالكترونية و اتجاه الفقه و القضاء بدأ ينحو إلى الاعتداد بصفة المنقول بهذه المعلوما ت، حيث يرون المعلومات أموال تصلح أن تنسحب عليها النصوص المتعلقة بالسرقة استنادا على كونها أصبحت محلا للتعاملات التجارية الحديثة[306].

و قد اتجه القضاء في بلجيكا و هولندا و المشرع الفرنسي إلى اعتبار المعلومات من قبيل الأموال التي تصلح لوقوع جريمة السرقة أو جريمة النصب[307].

و قد نصت محكمة النقض الفرنسية بتوافر خيانة الأمانة بخصوص رقم كارت السحب من البنك على سندات أحكام المادة 1/314 عقوبات تسري على كل مال أيا كانت طبيعته و ليس فقط على المال المادي[308].

"Les dispositions de l'article 314-1 du code pénal s'appliquent à un bien quelconque, et nom pas seulement à un bien corporel"

و في ذلك دلالة على اتجاه القضاء الفرنسي إلى التخفيف من الطابع المادي للمنقول محل جرائم الأموال ليكون له طابع معنوي مادام أنه له قيمة مالية و بذلك بشكل هذا الاجتهاد تطورا نحو الاعتراف بالمال المعنوي[309].

و قد تأثر المشرع الفرنسي بالاجتهادات القضائية و الآراء الفقهية في تعديله لقانون العقوبات سنة 1994 بنزوعه إلى الاعتداء بالأموال ذات الطبيعة المعنوية عندما استغنى عن الصياغة التقليدية "مال منقول مملوك للغير" محل لجرائم النصب و خيانة الأمانة

---

304 - علي عبد القادر القهوجي ، مرجع سابق ، ص 79.
305 - آمال 13، علي عبد القادر القهوجي ، مرجع سابق ، ص 80.
306 - شيماء عبد الغني ، مرجع سابق ، ص 38.

307 **Dominique DAVOUST, La lutte contre le blanchiment de capitaux : une action menée au plan international, européen et national , Revue petites affiches , Droit pénal des affaires, 05 août 2002 n° 155, P. 4**

308 - شيماء عبد الغني ، مرجع سابق ، ص 38.
309 - شيماء عبد الغني ، مرجع سابق ، ص 39.

بالصياغة "مال أيا كان أو خدمة"، كما وسعت المادة 1/313 عقوبات فرنسي في تعديل 1994 من مجال جريمة النصب فأصبحت تسري على الخدمات و ليس فقط على مال المنقول المملوك للغير[310].

المطلب الثاني : جريمة السرقة في مجال التجارة الالكترونية السرقة في نطاق المعلوماتية

الفرع الاول : مدى اعتبار البرنامج مالا بصدد جريمة السرقة

(دراسة) الوقوف على ماهية السرقة في مجال التجارة الالكترونية يتطلب بيان موضوعي و بيان أركانها للجريمة في نطاق المعلوماتية ذاتية خاصة[311].

فتتبعا للطبيعة الخاصة لتعاملات التجارة الالكترونية و التي ترد على منقولات ذات طبيعة معنوية تجعل من أركانها هذه الجريمة مفهوما مختلفا عما هو مقرر للمنقولات المادية[312].

01 -طبيعة المال في مجال التجارة الالكترونية:

أ/المعلوماتية مـــال: خالف أصحاب هذا الرأي غيرهم من الفقهاء الذين اعتبروا أن المعلومات

و اعترف هؤلاء بأن المعلوماتية مال لها قيمة مالية يمكن أن تخضع لأحكام السرقة. فالمعلومات في نظرهم هي "مجموعة من الأفكار متضمنة لرسالة يمكن إدراكها عن طريق النقل أو الحفظ أو المعالجة فالمعلومات تعتبر نتاجا ذهنيا لمبتكرها أو مبتدعها و يترتب على ذلك وجود علاقة بين هذه المعلومة و مبتدعها مثل تلك التي تنشأ بين المال و الشيء الذي يمتلكه، فيكون له نقلها و إيداعها و حفظها و تأجيرها و بيعها، فالمعلومة تعتبر أموالا لأنها ذات قيمة اقتصادية حيث أنها تطرح في الأسواق للتداول مثلها مثل أي سلعة كما أن لها سوقا تجاريا يخضع لقوانين السوق الاقتصادية"، فالمعلومة مجموعة مستحدثة من القيم مستقلة عن دعامتها المادية، و هي قيمة قابلة للاستحواذ تقوم وفق سعر السوق ترتبط بمنتجها بواسطة علاقة قانونية. تتمثل في علاقة المالك بالشيء الذي يملكه و منه فإنها تصلح لأن تكون محلا للسرقة[313].

---

[310] - شيماء عبد الغني ، مرجع سابق ، ص 40- 41.
[311] - حسام أحمد حسام طه تمام ، مرجع سابق ، ص 451.
[312] - شيماء عبد الغني ، مرجع سابق ، ص 44.
[313] أحمد خليفة الملط ، مرجع سابق ، ص 295.

من الآراء المؤيدة كذلك لاعتبار المعلوماتية مالا هي ملك التي ربطت بين الطبيعة المالية للمعلوماتية و بين الكيان المادي لها و حيث يرون أن المال المعلوماتي البرامج و المعلومات و إن كانت ليست شيئا ملموسا أو محسوسا إلا أنه يمكن أن يتجسد لها الكيان المادي باستظهاره على شاشة أو يترجم إلى أفكار أو أرقام تنتقل إلى الغير و بالتالي فهي لها كيان مادي[314].

و يرى فريق من الفقه أن المشرع في نصه عن أحكام السرقة (379 ع فرنسي/ 311 ع مصري) لم يذكر المال و لم يحدد طبيعته سواء كانت مادية أم معنوية و ترك الأمر للفقه و القضاء لتحديد الحكم و سمح لقضاء بأعمال سلطته التقديرية للقول بصلاحية الأموال المعنوية و قابليتها لأن تكون محلا للسرقة و أن تعد المعلومات أموالا و تخضع للقواعد العامة للسرقة، و هو ما نؤيده نظرا للفتحة التجارية و الاقتصادية لهذا النوع من الأموال[315].

02 -طبيعة المنقول في مجال التجارة الالكترونية:

المنقول هو ما له قيمة مالية و يمكن تملكه و حيازته و نقله من مكان إلى آخر[316].

أ/ المعلوماتية منقول:

يرى أصحاب هذا المذهب أن مصطلح الشيء الوارد في المادة 379 عقوبات فرنسي جديد تشمل الأشياء المادية و غير المادية، ما استدلوا على أن المعلوماتية منقول و تصلح أن تكون محلا للسرقة بالنصوص سالفة الذكر لا تحول من حيث المبدأ إمكانية وقوع السرقة على شيء معنوي فهي لم تشر إلى الشيء أو المال محل السرقة.

مما تبين أن طبيعة هذا المحل لا يرد عليها أي قيد أو تخصيص و السرقة و إن وقعت على أشياء مادية أو معنوية أمر سواء[317].

سند آخر و هو سرقة المعلومات و ليس الدعامات هي السبب في الجدل و الخلاف الفقهي فغير منطقي أن يهتم المشرع و يقر حماية للدعامات و يغفل أو يسكت عن تجريم سرقة المعلومات الموجودة بداخلها أو التي يمكن أن يحويها كالعبرة بالقيمة المالية و الاقتصادية و التجارية و النقدية لتلك المعلومات و الواقع الميداني يشهد أن

---

[314] - أحمد خليفة الملط ، مرجع سابق ، ص 296- 297.

[315] **Agathe LEPAGE, Réflexions de droit pénal sur la loi du 6 août 2004 relative à la protection des personnes à l'égard des traitements de données à caractère personnel,** Revue **Droit pénal n° 3, Mars 2005, Etude 5**

[316] - أحمد خليفة الملط ، مرجع سابق ، ص 298.

[317] - علي عبد القادر القهوجي ، مرجع سابق ، ص 86- 87.

القاضي لا يلتزم بحرمية النص لمنهج للتفسير بالمنطق العدالة و أسس التقاضي فقضى بأن يتعدى التفسير إلى غاية النص و منطقة مسايرة للتطور التقني، بمقتضيات حماية المجتمع تمنع أن تحرم سرقة الاسطوانة أو الدعامة ذات القيمة المهملة وفقا لحرمية النص و يسكت عن غايته و روحه بعدم تجريم محتوى الدعامة (معلومة، مال) الذي يجب حمايته فهو المقصود ابتداء من أحكام السرقة[318].

03 – ملكية الغير للمال (للشيء) المعلوماتي:

تضع القواعد العامة للسرقة شركات منقول بوقع جريمة السرقة، هما:[319]

عدم ملكية المال محل السرقة للسارق

ملكية المال محل السرقة للغير

و هذا تماشيا مع قصد المشرع من إقرار النص التجريمي حيث قصد حماية الملكية و ليس الحيازة، و التساؤل الذي يطرح هو هل الشيء أو المال هو الدليل ذاته على عدم ملكية الجاني له. ذهب جانب من الفقه إلى أن جوهر الاختلاس في السرقة هو دخول الشيء في حيازة الجاني (نص م 379 ع فرنسي، 311 ع مصري) و هو الشرط المفترض لوقوع السرقة على شيء منقول مملوك للغير و مثالها المعلومات باعتبارها ذات أهمية مالية نقدية تجارية اقتصادية[320].

و قد أكاد الفقه الفرنسي أن المشرع يعتد لملكية المعلومة للغير حيث عاقب على سرقتها، نفس تعريف المعلومة في الفقه هي كل رسالة يمكن نقلها للغير بأي وسيلة كانت. و وجود المعلومات سببه هو قابليتها للنقل للغير فقواعد حقوق الملكية تعترف بحق الملكية للمعلومات المسجلة على دعامة معالجة آليا لمن قام بالمعالجة الآلية لها، بالإضافة إل أن سرقة الدعامات المملوكة للغير و المسجلة عليها معلومات هي سرقة للمعلومات نفسها، حيث لا قيمة للدعامة دون معلومة، فالغرض من سرقة الدعامة هو

---

[318] - هدى حامد قشقوش ، مرجع سابق ، ص حامد، جرائم الحاسب الآلي، 67.

[319] - أحمد خليفة الملط ، مرجع سابق ، ص 203.

[320] **Dominique DAVOUST, La lutte contre le blanchiment de capitaux : une action menée au plan international, européen et national , Revue petites affiches , Droit pénal des affaires, 05 août 2002 n° 155, P. 4**

الاستحواذ على المعلومات و منه ينتقل الشيء المعلوماتي من حيازة مالكه إلى حيازة الجاني[321].

الفرع الثاني : مدى توافر أركان جريمة السرقة في مجال التجارة الالكترونية

.....

01 الركن المادي للسرقة في مجال المعلوماتية:

السرقة هي اختلاس من مال منقول مملوك للغير بنية تملكه (311 عقوبات مصري/ 1/311 عقوبات فرنسي) و سواء إن استولى الجاني على المال _ في فعل الاختلاس _ خلسة أو عنوة، أو تسلمه بناءا على يد عارضة فغير نيته و استولى عليه، و عليه فإن فعل الاختلاس يقتضي نقل حيازة المال موضوع الاختلاس أو السرقة من حيازة المجني عليه إلى الجاني[322].

و يرى جانب من الفقه أن الركن المادي في جريمة السرقة يتمثل في فعل الاختلاس و هو متكون من عنصرين موضوعي و آخر شخصي.

الموضوعي يتمثل في النشاط الإداري الذي يؤدي إلى النتيجة (سلوك نتيجة رابطة سببية)

و الشخصي تمثل في ..... الجاني في تملك الشيء و حيازته، و هو ما يعني عدم رضاء المجني عليه بخروج الشيء من حيازته.

يعني ذلك أنه من الممكن تطبيق هذه المبادئ العامة على سرقة الشيء المعلوماتي، ففعل اختلاس للمال أو الشيء المعلوماتي يتحقق بالنشاط و المادي الصادر من الجاني بتشغيل الجهاز و الحصول على البيانات أو المعلومات أو حيازتها أو الاستحواذ عليه دونما الحاجة لاستعمال العنت كما في الجريمة التقليدية. كي ينقل المعلومة و يستحوذ عليها، فهذا يحصل بفضل الشبكة و بسهولة دون الاضطرار لإثبات السلوك المادي المنصوص عليه في مواد السرقة بما فيها فعل الاختلاس للمنقول[323].

---

[321] – حسام أحمد حسام طه تمام ، مرجع سابق ، ص 483، الملط أحمد خليفة الملط ، مرجع سابق ، ص 304.

[322] – حجازي 192-193.

[323] **Christophe JAMIN, L'efficacité au service de la justice (*) , Revue Gazette du Palais, Procédure civile, 21 avril 2007 n° 111, P. 2**

فنتيجة فعل الاختلاس تتحقق بمجرد حيازة الجاني للمعلومة عن طريق استحواذها أو الحصول عليها بطريق غير مشروع فرابطة السببية..... متوافرة بين النشاط المادي الجرمي و النتيجة الإجرامية.[324]

و يشكل اختلاس المعلومة أو الشيء منفصلا عن دعامته المسجل عليها إشكالا كونه يصطدم مع المفهوم التقليدي الذي يقرر أن اغتصاب الحيازة لابد أن يكون نصبا مادي، كون الرأي المؤيد لسرقة الشيء المعلوماتي غير المادي تبنى تصورا قائما على إمكانية اختلاس المعلومات و البرامج مع إمكانية نقلها من حيازة الجاني إلى المجني عليه، فهذه الحيازة ترد على المعلومات محل السرقة مثلما ترد على المنقول المادي كل ذات الجريمة[325]، حيث البرامج و المعلومة هو خلق فكري، فتنقل الحيازة في السرقة المعلوماتية يكون من نفس طبيعة محل السرقة فهي حيازة فكرية و ليست حيازة مادية. فركن الاختلاس سيكون من نفس طبيعة الشيء أي الحيازة الفكرية لهذا الشيء المعلوماتي[326].

أما العنصر الشخصي في الحيازة أي عدم رضاء حائز الشيء في الحيازة المعلوماتية و المترتبة عن الاختلاس فتسعى أن مالك المعلومة أو حائزها أو صاحب الحق على الشيء المعلوماتي المعنوي لم يرضى باختلاس ما يخصه و لم يرضى بنقلها إلى الجاني، و إن افترض التسليم المسبق للشيء المعلوماتي فقد لا تعني الرضا بالاختلاس فقد كان ذلك بقصد تمكين اليد العارض و هذا لا ينفي ركن الاختلاس[327].

يتعين القول أنه لا مخالفة لمبادئ التفسير التي تحكم النصوص العقابية، أو مبدأ المشروعية ذلك لأن ثورة المعلوماتية أدت لإلى ظهور أنماط جديدة من الجريمة تعجز النصوص العقابية بأن تطالها بالمركز القانونية بالحماية، فمن باب الحفاظ على المصلحة العامة و الخاصة و لأجل نمو هذه التجارة الالكترونية يتعين التوسع في تفسير النصوص إلى أنه بصدد تشريع عقابي خاص يعنى بتنظيم هذه المسائل[328].

" و يمكن استخدام الوسائل الالكترونية كالحاسب في ارتكاب جرائم الاعتداء على الأموال حيث يمكن استخدامه في إدخال بيانات غير حقيقية أو تعديل البيانات الموجودة

---

[324] - هدى حامد قشقوش ، مرجع سابق ، ص حامد ح ح آ 61- 62، حسام أحمد حسام طه تمام ، مرجع سابق ، ص 462- 463، حجازي 193- 194.

[325] - حجازي 194.

[326] - هدى حامد قشقوش ، مرجع سابق ، ص حامد، جرائم الحاسب الآلي، 62.

[327] - حجازي 194. هدى حامد قشقوش ، مرجع سابق ، ص حامد ج ج آ 63.

[328] - حجازي 196.

أو مسح البيانات الموجودة و ذلك لاختلاس الأموال المادية أو لزيادة العناصر الإيجابية في ذمة الجاني فذلك يعد مرتكبا لفعل الاختلاس الذي يقوم به النشاط المادي لجريمة سرقة الشخص الذي يستعمل بيانات غير حقيقية أو يعدل في البيانات الصحيحة المتعلقة بمعاملة تجارية عبر الإنترنيت ليستولي على الأموال التي قام أحد المستهلكين بتحويلها لأحد الموردين للبضائع أو الخدمات و ذلك بإضافة هذه الأموال لحسابه الشخصي أو لحساب آخر، و لا يمكن القول بأن الجاني لم يسيطر على هذه الأموال فالحقيقة تثبت العكس حيث أنه أخرج هذه الأموال من ذمة المجني عليه و زاد بها العناصر الإيجابية لذمته المالية، كما لا يمكن القول بأنه قام فقط بالتلاعب في بيانات أو أرقام "[329].

02 –الركن المعنوي (القصد الجنائي) في سرقة الشيء المعلوماتي

يتمثل الركن المعنوي في القصد الجنائي (خاص و عام) بتوافر القصد العام في جريمة السرقة.

أ/ القصـــد العـــام: يتحقق القصد العام في السرقة بتوافر عنصرين العلم و الإرادة و ينصرف العلم إلى العناصر المكونة للواقعة الإجرامية حيث يعلم الجاني أن المال الذي يختلسه و ينقل حيازته من حائزه بدون رضاه ليدخله في حيازته هو أو تحت سيطرته. كما لابد أن ينتهي إلى علمه أن المال ليس ملكا له و أن تتجه إرادته إلى إلى ارتكاب فعل الحيازة و تحقيق النتيجة الإجرامية[330]

و المجرم المعلوماتي مرتكب لجريمة سرقة البرامج و المعلومات يسعى بإرادته إلى الاستحواذ عليها بتشغيله للجهاز و يعلم أنها مملوكة لغيره و في قيامه باختلاسها أو نسخها يعتبر قد توافر لديه عنصري القصد العام[331].

ب/ القصـــد الخـــاص:

جرائم (المعلوماتية التجارة الالكترونية) حديثة و هي جرائم متمثلة في الاعتداء على النظام المعلوماتي و ضمنها جرائم السرقة و هي جريمة عمدية و لا يكفي توافر القصد العام بل لابد من توافر القصد الجنائي الخاص و هو الذي يعبر عنه بنية التملك لأنها هي التي تكشف عن نية الجاني في حيازة الشيء المعلوماتي و يستدل على توافر القصد العام (العلم و الإرادة) فزيادة على ضرورة اتجاه إرادة الجاني إلى اختلاس الشيء

---

329 - مدحت رمضان عبد الحليم ، مرجع سابق ، ص148- 149، حجازي 197.

330 - أحمد خليفة الملط ، مرجع سابق ، ص الملط 335.

331 - هدى حامد قشقوش ، مرجع سابق ، ص حامد 63 ، أحمد خليفة الملط ، مرجع سابق ، ص الملط 336.

المعلوماتي و مع علمه بأنه يختلس شيئا مملوكا للغير فإنه يضاف إلى هذان العنصران عنصر نية الاستحواذ على الشيء المسروق[332].

و يجب أن تتوافر نية التملك و أن يتمكن و أن يكون هناك تزامن بين هذه النية و فعل الاختلاس الذي يقوم بالركن المادي للجريمة أما إذا كان القصد لاحقا فلا تقع الجريمة[333].

المطلب الثالث : موقف المشرع الجزائري

تضمنت المادة 356 من قانون العقوبات الجزائري فعل الاختلاس بنصها على أن " كل من اختلس شيئا غير مملوك له يعد سارقا " و من استقراءنا النص نجد أن المشرع الجزائري كان أكثر ليونة في نصه على فعل الاختلاس و هذه الليونة دفعت بأعمال الاجتهاد القضائي إلى مراعاة الظروف و الوقت التي صدرت فيها نصوص السرقة التي ركزت حمايتها الجنائية على الأموال المنقولة المادية. لكنها في نفس الوقت لا تحول دون إمكانية تطبيق نصوص السرقة على كل الأشياء المعنوية بمصطلح شيء ليس له دلالات الأشياء المادية فحسب بل يشمل كذلك الأشياء المعنوية فطبيعة الشيء محل السرقة غير محددة في نص المادة 350 ع ج، و فيهما سبق و أن شرحنا من كون الأشياء المعنوية أي المعلومات و البرامج من تقبلها للتملك و الحيازة و النقل فهي تصلح لأن تكون محلا لجريمة السرقة دون أن يكون ذلك خروجا عن مبدأ الشرعية و هذا التفسير مبرر لسببين[334]:

نصوص السرقة لا تحدد صفة الشيء محل الجريمة محل الجريمة مادي أو معنوي.

الأشياء المعنوية يصدق عليها وصف المال (قيمة تجارية و اقتصادية)

و بذلك فإن القاضي الجزائي الجزائري يمكن له أن يطبق أحكام السرقة على أموال التجارة الالكترونية و إن كان البعض يفضل أن ينص التشريع الجزائري على اعتبار المعلومات و المعطيات أحد عناصر الذمة المالية و تجرم الاعتداءات التي تقع عليها، أو أن تحذو حذو تشريعات أخرى في إعطاء مفهوم موسع المال و عرفته بأنه كل شيء له قيمة مالية، و يدخل فيه تبعا لذلك الأشياء المعنوية و المعلومات و المعطيات التي

---

[332] - هدى حامد قشقوش ، مرجع سابق ، ص حامد 63، الملط ناقل 336- 337.

[333] - حسام أحمد حسام طه تمام ، مرجع سابق ، ص 515.

[334] - آمال قارة ،مرجع سابق ، ص 28- 29.

تمت معالجتها آليا و أقرت صلاحيتها لأن تكون محلا لجريمة السرقة فمثلها بالحماية الجنائية[335].

مدى صعوبة تطبيق الجزاء في سرقة الشيء المعلومات المعنوي[336]

مدى فاعلية الجزاء في سرقة المال المعلوماتي المعنوي[337]

المطلب الثالث : جريمة النصب في مجال التجارة الالكترونية

مدى اعتبار المعلوماتية مالا بصدد جرائم النصب

تعد جريمة النصب أنسب الجرائم في تكيفها على تجريم الاعتداءات الواقعة على نظم و أموال التجارة الالكترونية لأن جريمة النصب يرتفع فيها مستوى الذكاء بهدف الاستيلاء على المال برضاء معيب و ذلك باستخدام الطرق الاحتيالية كالتدليس و الخداع لإيهام المجني عليه.

و المشرع الفرنسي توسع في مفهوم المال[338] محل التسليم في جريمة النصب في المادة 1/313ع ف حيث نصب على أنه محل النصب قد يكون نقودا أو قيما أو أموالا أو تقديم خدمات و الرضا بعمل يفرض التزاما أو إعفاء، و حسب رأي البعض فإن المشرع قد تخلى عن لفظ الأشياء لئلا تنصرف إلى الأموال المادية المنقولة و استعمل لفظي نقود و أموال حتى يمكن إدخال الأموال المعنوية ضمن الأموال التي تكون محلا لجريمة النصب فلا يشترط في المال بالضرورة أن يكون من الأموال المادية[339].

أما بالنسبة للمشرع الجزائري فإن السؤال المطروح هو (أو يطرحه النص) [340] مدى إمكانية أن تطال نص المادة 372 ع ج بحماية المعلومات و البرامج المتعلقة بالتجارة الالكترونية[341].

الفرع الأول: جريمة النصب المعلوماتي في التشريعات المقارنة:

تنازعت هذه المسألة عدة اتجاهات هي:[342]

---

[335] - آمال قارة ،مرجع سابق ، ص 29- 30.

[336] - هدى حامد قشقوش ، مرجع سابق ، ص حامد ج ح آ 64- 68

[337] - هدى حامد قشقوش ، مرجع سابق ، ص حامد ج ح آ 69- 73.

[338] **Christophe CARON, Vers un droit pénal communautaire de la contrefaçon, Revue Communication Commerce électronique n° 6, Juin 2007, Repère 6**

[339] - مدحت رمضان عبد الحليم ، مرجع سابق ، ص144.

[340] - حجازي 215.

[341] - آمال قارة ،مرجع سابق ، ص 30.

[342] - حجازي 217.

01- الاتجاه الأول: يرى أن جريمة النصب لا تقع إلا إذا خدع الجاني إنسانا مثله، و أن يكون الشخص المخدوع مكلفا بمراقبة البيانات، و منه لا ينطبق النص الجنائي للنصب لعدم تصور خداع الحاسب الآلي لأنه ليس بشخص.

02- الاتجاه الثاني: تبنته الدول الانجلوسكسونية و هذا التجاه وسع من نطاق التجريم في النصوص الخاصة بجريمة النصب لتشمل النصب المعلوماتي و من الدول التي تبنت هذا الاتجاه بريطانيا، استراليا، كندا و القضاء في هذه البلدان لم يخرج على نصوص القانون في تجريمه للنصب المعلوماتي ذلك أن المشرع عندهم نص على قواعد و نصوص تجريمية لهذه الجريمة بقي للقضاء نقط تكييف الواقعة و تطبيق النص عليها[343].

03- الاتجاه الثالث: و تمثله الولايات المتحدة الأمريكية فقد أصدرت بعض ولايتها أصدرت قوانين أضافت فيها تعاريفا موسعة للأموال بأنها "كل شيء ينطوي على قيمة". و بذلك اندرج تحت مسمى هذه الأموال الأموال المعنوية و البيانات المعالجة فعاقبت هذه القوانين على الاستخدام غير المسموح به للحاسب الآلي بغرض اقتراف أصحاب الغش أو الاستيلاء على الأموال[344].

04- الجهـــود التشريعيـــة:

قدمت الحكومة الأمريكية في أوت عام 1984 مشروعا لقانون يجرم الغش المعلوماتي يعاقب فيه كل من رتب أو صمم خطة ما أو حيلة بغرض ارتكاب غش أو الاستيلاء على مبلغ من النقود أو مالا لا يخصه و ربح أو حاول الولوج في حاسب آلي لأجل محاولة أو تنفيذ حيلة أو محاولة أو ارتكاب مثل هذا النصب أو هذه السرقة أو الاختلاس[345]

تدخل المشرع الانجليزي سنة 1983 بعدما تردد الفضاء الانجليزي في تطبيق نصوص السرقة التي هدرت سنة 1978 و التي عاقبت كل من حصل على مال الغير أو منفعته بطريق الغش و الخداع و دفع ذلك المشرع إلى اعتبار خداع الآلة بنية ارتكاب غش مالي هو من قبيل الاحتيال الذي يجب العقاب عليه جنائيا.

---

[343] - آمال قارة ،مرجع سابق ، ص 47، بالنصوص الواردة المتعلقة بالنصب ذات طابع متسم بالعموم و الشمول حيث يمكن الاستناد على هذه السمة ليشمل تطبيق أحكام هذه النصوص على فعل الاحتيال على الحاسب و أن تطال نصوص النصب معاملات التجارة الالكترونية، آمال قارة ،مرجع سابق ، ص 47.

[344] - حجازي 220- 221.

[345] - و المال حسب النص الذي ورد في هذا المشروع هو "كل الوسائل المالية و المعلومات التي تحتوي على بيانات معالجة و المكونات الالكترونية و الكيانات المنطقية و برامج الحاسب الآلي سواء بلغة الآلة أو بلغة مقروءة للإنسان، و كل قيمة أخرى ذات طابع حادي أو معنوي"، حجازي 222.

و بذلك أصبح القضاء في إنجلترا يطبق نصوص تجرم النصب إذا تعلق بذلك النوع من الغش أو الاحتيال بطرق معلوماتية و كذلك القضاء الكندي و الاسترالي[346].

الفرع الثاني : مدى توافر أركان جريمة النصب في مجال التجارة الالكترونية

01- الركن المادي لجريمة النصب في مجال التجارة الالكترونية:

يقوم الركن المادي في جريمة النصب على فعل الاحتيال و تسلم المال و علاقة السببية التي تربط بينهما و إن كان الجدل قد ثار في الفقه _ و لن يستمر _ حول صلاحية المعلومة أو البيانات كي تكون محلا لجريمة النصب إذ كانت مستقلة عن دعامتها المادية فإنه و بالرجوع لنص المادة 372 عقوبات جزائري التي نصت على "كل من توصل إلى استلام أو تلقي أموالا منقولة أو سندات أو تصرفات أو أوراق مالية أو وعود أو مخالصات أو إبراء من التزامات أو الحصول على أي منها أو شرع في ذلك و كان ذلك بالاحتيال..." فليس هناك ما يحول دون وقوع المعلومات أو البرامج أو الأموال المعنوية تحت طائلة تجريم هذا النص باعتبارها أموالا أو منقولات أو إبراء الالتزام أو الحصول عليها أو تصرفات..[347]

يقوم الركن المادي في جريمة النصب على فعل التدليس و تسلم المال، و علاقة السببية إلا أن الفقه يثير التساؤل عن مدى توافر أركان جريمة النصب في نطاق التجارة الالكترونية من يتمكن تخص من الوصول إلى نظم المعلومات المعالجة الكترونيا إلى الاستيلاء على مال الغير فلو افترضنا تخص قام بالتلاعب في بيانات بنكية و قام بتحويلات باسم كاذب أو صفة غير صحيحة فالمعيار في ذلك هو المحاولة التدليسية و هو المعيار الأساسي لجريمة النصب[348].

و توجد أساليب فنية يستخدمها الجاني و مرجع ذلك إلى الطبيعة الذاتية لجريمة النصب المعلوماتي حيث تتوافر الخبرة الفنية في خداع الحاسب الآلي و كيفية الحصول على الهوية و اختلاسهاو انتحال صفة صاحبها للحلول محله في العمليات الالكترونية، و باختلاس الهوية يمكن الحصول على المستخرجات و نتائج العملية الآلية[349].

أ/ فعـــل الاحتيـــال:

---

[346] - حجازي 219- 220.

[347] - آمال قارة ،مرجع سابق ، ص، 31.

[348] - حسام أحمد حسام طه تمام ، مرجع سابق ، ص 521.

[349] - حسام أحمد حسام طه تمام ، مرجع سابق ، ص 522، ينبغي الرجوع ضرورة إلى أحمد خليفة الملط ، مرجع سابق ، ص الملط 402و ما بعدها الاحتيال على النظام المعلوماتي413-422 و مابعدها التسليم الواقع بواسطة الأنظمة المعلوماتية.

و لكون الركن المادي في جريمة النصب يعتبر جوهر الجريمة فإننا سنعرض لفعل الاحتيال لم يورد المشرع تعريفا محددا للطرق الاحتيالية و ترد ذلك لاجتهاد الفقه و القضاء و العلة في ذلك لدى البعض أن كل تعريف يقصر عن الإحاطة بأساليب الاحتيال المتقنة و المتطورة، و يشترط لتوافره ما يلي:

أ- أن تأتي الجاني طريقا يرتقي لأنه يصنف احتياليا فكل ضرب من الغش لا يعد طرقا احتياليا لا يرتقي إلى درجة التدليس الجنائي.

ب- أن ينصرف غاية الجاني من استعمال تلك الطرق إيهام المستهلك و في إطار العلاقة التعاقدية التجارية بوجود مشروع كاذب أو واقعة ضرورة لإحداث الأمل بالحصول على ربح وهمي أو تسديد مبلغ ما أو إيهامه بوجود سند دين غير صحيح أو سند مخالصة مزور أو أي تصرف أورده المشرع مصرا في النص الخاص بالنصب[350].

و نظرا لفقه فإن الاحتيال لا يقوم بمجرد الكذب العادي أو كتمان أمر من الأمور التي يجب التصريح بها بل يجب أن يدعم الكذب بوقائع مادية أو مظاهر خارجية توصى بصدق إدعاء الجاني و تدفع المجني عليه لانطلاء الكذب عليه.

و قضت محكمة النقض المصرية بأن الكذب لا يرتقي إلى درجة الاحتيال إلا إذا اصطحبت بأعمال خارجية و مادية تحمله على الاعتقاد بصحته ثم تحمله على الاعتقاد صحيحة ثم تسلم المال و بذلك يحصر لجريمة النصب ثلاث شروط:[351]

1- الكذب

2- المظاهر الخارجية

3- غاية الطرق الاحتيالية

ب/ فعل الاستيلاء على مال الغير/ التسليم الالكتروني:

لتقوم جريمة النصب يتعين أن يترتب على فعل الاحتيال أن يستولي الجاني على أموال الغير دون وجه حق و أدائه في ذلك الجهاز الحاسب الآلي كأداة إيجابية في هذا الإستيلاء حتى تم الدخول مباشرة في المعطيات، و في الكيان المنطقي و المتمثل في إدخال معطيات وهمية أو بتعديل البرامج أو خلق برامج صورية[352].

---

[350] - أحمد خليفة الملط ، مرجع سابق ، ص الملط 369.

[351] - أحمد خليفة الملط ، مرجع سابق ، ص الملط 370/369.

[352] - حجازي 223.

و النتيجة التي أرادها المشرع لتمام جريمة النصب هي التسليم و تتحقق بتوصل الجاني إلى الإستيلاء على مال الغير من نقود و عروض تجارة أو سندات دين أو سندات مخالصة، و يعطى لفظ التسليم دلالة أكبر في جريمة النصب المعلوماتي فالمجني عليه يقوم بتسليم المال تحت تأثير الغلط الذي أوقعه فيه الجاني فمعيار التسليم هو إرادة المجني عليه المعينة بالتدليس و هي تعني تمكين التهم من السيطرة على مال سواء تمت هذه السيطرة فورا أو بعد وقت كما في التحويلات البنكية و الأرصدة[353].

ج/ علاقـــة السببيـــة:

يلزم في جريمة النصب أن يكون التسليم قد وقع كأثر من آثار الطرق الاحتيالية المستخدمة من الجاني، حيث يعني علاقة السببية أن يكون الاحتيال هو الدافع على التسليم و هو ما يوجب على قاضي الموضوع أن يستظهر الصلة بين وسيلة الاحتيال الذي استخدمها الجاني و من تسلم المجني عليه للمال[354].

و يتطلب لقيام علاقة السببية بهذا المعني عند الفقه و القضاء:

- أن يكون التسليم لاحقا على فعل التدليس
- أن يتم التسلم بناءا على غلط
- أن يكون التسليم نتيجة لانخداع المعنى
- الشروع في النصب[355].

و علاقة السببية عنصر لازم لتمام ماديات جريمة النصب لإسناد الاستيلاء على المال إلى احتيال الجاني، فالطرق الاحتيالية التي اتخذها الجاني ترتبط بينها و بين المال المسلم علاقة هي السبب في هذه الجريمة، و لولا هذه الطرق الاحتيالية لما تمت الجريمة التي أوقعت المعني عليه في الفخ و جعلته يسلم ما له سواء أكان شخصا أو آلة حيث التحايل على الآلة يكون بعدة طرق كأن يستخدم مستندات مستخرجة من الحاسب وهمية توحي بوجود مشروع كاذب أو سند دين و همي كون الحاسب يعطي الثقة في المعاملة و خداع الآلة هو خداع لصاحبها في الواقع[356].

---

353 - حسام أحمد حسام طه تمام ، مرجع سابق ، ص 514 بتفصيل.
354 - أحمد خليفة الملط ، مرجع سابق ، ص الملط 389.
355 - للإطلاع أكثر أنظر أحمد خليفة الملط ، مرجع سابق ، ص الملط 389- 390.
356 - حسام أحمد حسام طه تمام ، مرجع سابق ، ص 548- 549.

ملاحظـــة: وفقا لنص المادة 1/313 من قانون العقوبات الفرنسي الجديد عدا أنه امتعاض بلفظ النقود و الأموال لمحل لجريمة النصب عن لفظ الأشياء الواردة في المادة 405 في القانون القديم.

لكون الأموال وقع على تكييفها القانوني تطور حيث لم يعد يشترط في الأموال أن تكون دائما مادية إلا أن الأموال وقع على تكيفها القانوني تطور حيث لم يعد يشترط في الأموال أن تكون دائما مادية إلا أن السبق الذي أقره المشرع هو اعتبار الخدمات محلا لجريمة النصب و تطالها النصوص الجنائية فالجريمة تقع إذا كان محلها خدمة من الخدمات فاعتبر تقديم خدمة بناءا على النشاط الإجرامي من الجاني مكونا لجريمة النصب وقد كانت معتبرة محلا لجرائم الأموال وفق ما استقر عليه الفقه التقليدي و القضاء لعدم وجود كيان مادي للخدمة [357]وهذا التعديل الذي أدخله المشرع الفرنسي بعد تجديدا أساسيا نحوى تجريم النصب فضلا من الخدمات لا يعد سرقة,إلا أن استخدام الطرق لاحتياله والحصول على صدقة يعد مكونا لجرعة النصب وفقا للتعديل الأخير وهذا التعديل الذي ادخله المشرع الفرنسي يعد تجديدا أساسيا نحوى تجريم النصب فاختلا بين الخدمات لا يعد سرقة, إلا استخدام الطرق الاحتيالية والحصول على صدقة يعد مكونا لجرعة النصب وفقا للتعديل الأخير وهذا ما ندعو المشرع الجزائري إلى اعتباره في تكيف عناصر جرعة النصب محكما المثير الرخاء بعمل مرتب التزاما أو إعفاءا فدخل في نطاقه التجريم عقود البيع أو القرض صالحا أنه قد تم حمل المجني عليه على الرضاء بالتعاقد مؤثر للطرق الاحتيالية المستخدمة من قبل الجاني بالرغم من توازن العقد[358]

02- الركـــن المعنـــوي

جريمة النصب جرعة عددية تتطلب لقيام ركنها المعنوي قصدا جنائيا ثم قصدا جنائيا خاصا.

ويحقق القصد العام إذ علم المتهم أنه يرتكب فعل قد ليس من شأنه أن يوقع لمجني عليه نحوى الغلط الذي حمله على تسليم ماله (وتنصرف إرادته) ولا يكفي أن يكون الجاني عالما فقط باحتياله ولكن لا بد أن تكون غايته من وراء الاحتيال هي أن يسلب جزءا من مال الغير أو عليه كليا بنية حرمانه نهائيا[359]

---

[357] - مدحت رمضان عبد الحليم ، مرجع سابق ، ص144 حجازي 225.

[358] - مدحت رمضان عبد الحليم ، مرجع سابق ، ص145

[359] - حسام أحمد حسام طه تمام ، مرجع سابق ، ص 549.

أما القصد الخاص فهو نية التملك إي انصرف فيه الجاني وهدفه هو الاستيلاء على مال مملوك لغيره من هذا الاحتيال ومن صوره استخدام صاحب البطاقة مع علمه أن رصيده غير كافي واستخدامها لأجل الحصول على مبلغ وخدمات أو أن يستخدم سارق البطاقة استعمالها للحصول على مبلغ أو خدمات وهو عالم بأنه لا حق له في ذلك [360] فنية التملك موجود عند الشخص الذي يستخدم بطاقة مزورة أو مسروقة وهو عالم بأنه سلب لمال الغير باتخاذ اسم كاذب بطرق احتيالية على الجهاز أو بتقديم بطاقة للشراء أو التوقيع على فواتير الشراء باسم كاذب بانتحال صفة الغير فهذه النية يتوافر بها القصد الجنائي لجريمة النصب في معاملات التجارة الإلكترونية[361].

المطلب الرابع : جريمة خيانة الأمانة في معاملات التجارة الالكترونية:

حددت المادة 376 من قانون العقوبات الجزائري محل جريمة خيانة الأمانة. بأنه أوراق تجارية، نقود، بضائع، أوراق مالية أو مخالصات أو محررات تثبت التزاما أو إبراء. بينما حددت المادة 1/314 من قانون العقوبات الفرنسي محل جريمة خيانة الأمانة بأن النقود أو القيم أو الأموال.

و يثور التساؤل و التساؤل القائم هو حول مدى إمكانية تطبيق نصوص خيانة الأمانة على جرائم التجارة الالكترونية حيث الطبيعة غير المادية للقيم في مجال الجريمة المعلوماتية في حد ذاته تعد إشكالا كون جريمة خيانة الأمانة ترد على منقول مادي لكن بعض القيم مثل البرامج و المعلومات أو المعطيات تصلح أن تكون محلا لخيانة الأمانة بوصفها بضائع، و أساس ذلك أن لها قيمة ذاتية يمكن أن تقدر فيطلق عليها مفهوم البضاعة و هو ما أخذ به المشرع الفرنسي[362].

و مع ذلك تساءل الفقه عن إمكانية وقوع جريمة خيانة الأمانة المعلوماتية أي مدى اعتبار البرامج و المعلومات محلا لجريمة خيانة الأمانة.

الفرع الأول: إمكانية وقوع جريمة خيانة الأمانة المعلوماتية:

فيصور وقوع جريمة خيانة الأمانة في نطاق التجارة الالكترونية كما لو تسلم الجاني من المجني عليه برامج أو معلومات المسجلة على دعامات. على أن يردها إلى المجني عليه بمقتضى عقد من العقود التي نص عليها القانون، بعدها قام المجني عليه بمقتضى عقد من العقود التي نص عليها القانون، بعدها قام الجاني بنقل الحيازة الناقصة إلى

---

[360] - حجازي 228.

[361] - أحمد حسام طه تمام ، مرجع سابق ، ص حسام 551.

[362] - آمال قارة ،مرجع سابق ، ص 31- 32.

حيازة كاملة بأن تصرف في البرامج تصرفا تصرفا أدى إلى هلاك الأخيرة و استعملها _ كما لو كان هو صاحبها _ استعمالا لم يتفق عليه أو قام بتبديدها أو إعارتها على غير المتفق عليه[363].

أما بالنسبة للفقه المصري يرى جانب منه [364] بأنه الأموال غير المعنوية تصلح لأن تكون محلا لجريمة خيانة الأمانة و ذلك استقراء لنص المادة 341 من قانون العقوبات المصري حيث أشار المشرع في نصها "مبالغ أو أمتعة أو بضائع أو نقود أو تذاكر أو كتابات أخرى مشتملة على شيك أو مخالصة أو غير ذلك". فالأموال المادية قد نص عليها المشرع ثم أضاف عبارة أو غير ذلك و هذا اللفظ فسره الفقه في مصر على أنه معناه الأشياء الأخرى التي لها قيمة غير مادية و عليه تصلح المعلومات و البرامج و كل مستخرجات الحاسب الآلي لئن تكون فاعلا أو موضوعا لجريمة خيانة الأمانة[365].

أما القضاء الفرنسي فقد اجتهد في إنزال فكرة خيانة الأمانة في مجال المعلوماتية على لفظ "البضائع" و "المحررات" أي أنه قال بوقوع جريمة خيانة الأمانة بطريقة معلوماتية.[366]

و فكرة "البضائع" تعني أن أيما نتاج طبيعي أو اصطناعي من صنع الإنسان يمكن أن يكون محلا للتجارة أو أن يستخدم عمليات تجارية و هو ما جعل القضاء يستقر على أن المحرر و لو لم يشمل على تمسك أو مخالصة لكن قيمته الكبيرة هو من قبيل البضائع حسب نص المادة 1108 من القانون المدني[367].

و قد قضت المحاكم الفرنسية بأن كل الأوراق التي لها قيمة يمكن تقديرها بالنقود تعتبر بمثابة بضائع كالتصميمات الهندسية، و المستندات المتعلقة بعملاء مكتب متخصص في الخبرة المحاسبية دون أن تكون مرتبة التزاما أو مخالصة[368].

و قد يكون من قبيل الغش المعلوماتي الجرم بخيانة الأمانة عندما يقوم المبرمجون بتسجيل المعلومات التي يحصلون عليها عن طريق التعدي على أنظمة المعلومات و

---

[363] - حسام أحمد حسام طه تمام ، مرجع سابق ، ص 558، حجازي 240 **Agathe LEPAGE, Libertés sur l'Internet et cybercriminalité : les apports au droit pénal de la loi pour la confiance dans l'économie numérique du 21 juin 2004, Revue Droit pénal n° 12, Décembre 2004, Etude 18**

[364] - حسام أحمد حسام طه تمام ، مرجع سابق ، ص 559، حجازي 241.

[365] - حسام أحمد حسام طه تمام ، مرجع سابق ، ص 559.

[366] - حجازي 241.

[367] - حجازي 241- 242.

[368] - حجازي 242.

بنية استخدامها في أغراض غير مشروعة كون البيانات و الكيانات المنطقية تصنف من قبيل المعلومات المعالجة، و التي لها قيمة تجارية، و لذلك يمكن وصفها أموالا[369].

و في كثير من حالات التلاعب في مرحلة إدخال البيانات إلى الحاسب الآلي أو في مرحلة البرمجة يلجأ القضاء الألماني إلى الاستعانة بجريمة خيانة الأمانة طالما أنها تتم داخل منشأة بمعرفة مستخدميها أو عن طريق مبرمجين تربطهم علاقة تعاقدية برب منشأة العمل[370].

الفرع الثاني : السلوك الإجرامي المعلوماتي في جريمة خيانة الأمانة:

نستعرض تلك الأفعال

يتحقق الفعل الإجرامي بقيام الركن المادي للجريمة. و هو يتمثل في قيام الجاني بتصرفات الاختلاس و التبديد أو استعمال الشيء.[371]

01- الاختـــلاس:

يتحقق فعل الاختلاس المعلوماتي في جريمة خيانة الأمانة بتصرف الأمين تصرفا يعبر فيه عن اتجاه نيته على إضافة المال إلى ملكه و أن يحل محل صاحبه دون أن يرتب ذلك خروج المال من حيازته[372] حيث المستفاد من

و يعرف أيضا بأنه يتحقق في حالة ضم الشخص المال الذي ائتمن عليه إلى ملكه و يقوم بالتصرف فيه تصرف مالكه الأصلي و يعني الاختلاس كمعيار هو تغير إرادة الجاني من أمين على المال المؤتمن عليه إلى بنية تملكه لنفسه بناءا على عقد من عقود الأمانة فتحول الحيازة الناقصة إلى حيازة (كاملة) تامة و ضابط التفريق بين مفهوم الاختلاس في السرقة و جريمة خيانة الأمانة، غير أن الاختلاس في جريمة السرقة يقع دون رضاء المالك، فهو سلب لحيازة الشيء بركنيها المادي و المعنوي أما في جريمة خيانة الأمانة فالتسليم يكون بناءا على عقد من عقود الأمانة الذي يليق الحيازة مؤقتة أو ناقصة بعدها تتحول نية (الجاني المختلس) إلى تملك الشيء لنفسه[373].

و عادة ما تقع أفعال الاختلاس المعلوماتي في جريمة خيانة الأمانة في الغش المحاسبية و يستخدم فيها الحاسب الآلي لأجل إخفائها.

---

369 - حجازي 243.
370 - حجازي 243.
371 - حسام أحمد حسام طه تمام ، مرجع سابق ، ص 563.
372 - حجازي 244.
373 - حسام أحمد حسام طه تمام ، مرجع سابق ، ص 563.

و يرى الفقه الجنائي أنه يتصور وقوع بالنسبة للأشياء غير المجسمة المتعلقة بالمعلومات الاختلاس المعلوماتي و خاصة الأمانة في التشريع الفرنسي بالنسبة للدعامات التي تحوي بيانات و برامج حتى سلمت للجاني بناء على عقد من عقود الأمانة حيث هي بمثابة أقوال مادية فنقول و تصلح لأن تكون محلا لجريمة خيانة الأمانة[374].

02- التبديـــد:

يقوم التبديد بفعل إعدام أو إتلاف الشيء الذي ائتمن عليه الجاني باعتباره مالكا أو القيام ببيع أو إعطاءه لشخص آخر فيخرجه من حيازته كله أو بعضه[375].

و يتصور وقوع التبديد في نطاق التجارة الالكترونية في حالة تسلم الجاني بناءا على قد من عقود الأمانة برام ج أو دعامات معلوماتية ثم يقوم باستعمالها على نحو يؤدي إلى تبديدها[376] و هذه الواقعة متصورة في حالة المنافسة غير المشروعة باستئجار نضم مستخدمين مؤسسة منافسة.

و التبديد يقع على النظام المعلوماتي من مكونات مادية و معنوية باعتبارها أموالا منقولة[377].

03- الاستعمـــال:

الاستعمال هو ذلك الفعل الذي يستخدم به الجاني المال المسلم إليه إلى درجة إعدام المال قيمة و استنزافه كله أو جزء منه مع بقاء مادة المال على حالها و يتحقق ذلك عندما يكون استعمال الشيء مخالفا للغاية التي خصصت من أجله [378] و قد قضى القضاء الفرنسي بوقوع جريمة خيانة الأمانة في قضية قام الأمين بتسليم الغير عدة شرائط ممغنطة تحوي مجموعة أغاني كي يسجلها ثم يعيدها إلى مكانها[379].

و مثالها أن يسلم مهندس تصميما لأحد المتعاملين الملاك خاص بمنزل يراد إنشاءه قصد الاطلاع عليه و بدون علم المهندس ينسخ المالك صورة عن التصميم و رد الأصل إلى صاحبه[380].

---

374 - حسام أحمد حسام طه تمام ، مرجع سابق ، ص 564، حجازي 246.
375 - حسام أحمد حسام طه تمام ، مرجع سابق ، ص 565.
376 - حجازي 247، حسام أحمد حسام طه تمام ، مرجع سابق ، ص 566، أحمد خليفة الملط ، مرجع سابق ، ص الملط 492.
377 - أحمد خليفة الملط ، مرجع سابق ، ص الملط 492.
378 - أحمد خليفة الملط ، مرجع سابق ، ص الملط 492.
379 - حجازي 248.
380 - الملط أحمد خليفة الملط ، مرجع سابق ، ص 492.

من صور جريمة خيانة الأمانة في مجال التجارة الالكترونية إذا ما قام موظف مسؤول عن التحويلات الالكترونية في مؤسسة حالية ما بظهور على مال أحد عملاءها و تصرف فيها تصرف المالك عد فعله خيانة أمانة.

أو إذا ائتمن شخص على صور او أفكار أو برامج للحساب و قام الأمين عليها بنسخها و استعمالها بمقابل عبر الإنترنيت فلدى البعض يرى بأن هذا الفعل لا يشكل جريمة خيانة أمانة لكن في نظرهم يقع هذا الفعل تحت طائلة نصوص عقابية أخرى كقواعد حماية الملكية الفكرية و الأدبية[381].

إلا أن البعض يرى أن هذا الفعل يشكل جريمة خيانة الأمانة في مجال التجارة الالكترونية إذا ما قام موظف مسؤول عن التحويلات الالكترونية في مؤسسة حالية ما بظهور على مال أحد عملائها و تصرف فيها تصرف المالك عد فعله خيانة أمانة.

أو إذا ائتمن شخص على صور أو أفكار أو برامج للحساب و قام الأمين عليها بنسخها و استعمالها بمقابل عبر الإنترنيت فلدى البعض يرى بأنه هذا الفعل لا يشكل جريمة خيانة أمانة لكن في نظرهم يقع هذا الفعل تحت طائلة نصوص عقابية أخرى كقواعد حماية الملكية الفكرية و الأدبية.[382]

إلا أن البعض يرى أن هذا الفعل يشكل جريمة خيانة الأمانة و المقصود من الاستعمال في هذه العناصر الحالة هو ..... إلى إفقاد الشيء قيمته كليا أو جزئيا و هو ذاته المعنى في الجريمة فكون الجاني قد أساء استعمال الأشياء المسلمة ..... على سبيل الأمانة و ذلك بنسخها [383] وهذه صورة الركن المادي لجريمة خيانة الأمانة و قد سلك القضاء الفرنسي ملك الفقه في التوسع أما القضاء فسلك مسلك الفقه في التوسع في جريمة خيانة الأمانة و قضى بأن هذه الجريمة تنشأ عن الاستخدام المتعسف في استعمال سلطة في أغراض أجنبية عن تلك المشترطة في العقد[384].

فقد قضى بأن الاختلاس ناشئ من عدم مراعاة الالتزامات المفروضة على مستلم الشيء التي بمقتضاها تم تسليم الشيء إليه و انتهاك عقد الأمانة لا يعد سببا مباشرا لوقوع الجزاءات الجنائية فهذه مسألة تخص القانون المدني لكن اختصاص القانون الجنائي يطال الأفعال التي هي من قبيل أفعال الغش385.

---

381 - مدحت رمضان عبد الحليم ، مرجع سابق ، ص154.

382 - مدحت رمضان عبد الحليم ، مرجع سابق ، ص154.

383 - حجازي 251.

384 - الملط 512-513.

385 - أحمد خليفة الملط ، مرجع سابق ، ص الملط 513.

الفرع الثالث :موقف الأنظمة القانونية المعاصرة من جريمة خيانة الأمانة في مجال المعلوماتية:

يرجع إلى خليفة الملط، الجرائم المعلوماتية، ص 505– 517.

المبحث الثاني : الجرائم الواقعة على التوقيع الالكتروني

المطلب الأول : الإطار القانوني للتوقيع الإلكتروني

لم يصبح التوقيع التقليدي وسيلة عملية وفي إطار إثبات التصرفات القانونية (في شكل إمضاء أو ختم أو بصمة) بالإضافة إلى كون وسيلة غير ملائمة للمعاملات المالية أو التجارية التي تتم عن طريق الكتابة الإلكترونية والمحررات الإلكترونية نظرا كبديل للتوقيع التقليدي توقيع أكثر ملائمة مع المعادلات الحديثة وآلياتها وهو التوقيع الإلكتروني.

الفرع الأول : ماهية التوقيع الإلكتروني

تصدت كثير من المنظمات لتعريف التوقيع الإلكتروني من خلال قوانين الإلكترونية وتشريعات التجارة الإلكترونية وأحيانا قوانين خاص بالتوقيع الإلكتروني ولعل أبرز هذه المنظمة . علاء نصيرات 23.

منظمة الأمم المتحدة . لجنة الأمم المتحدة للتجارة الدولية (الأوسترال) كمظمة دولية.

الإتحاد الأوروبي لمنظمة سليمة.

01- تعريف التوقيع الإلكتروني في التشريعات المقارنة:

عرف المشرع الفرنسي في المادة 1916 من التقنين المدني المعدل والمضافة بقانون 13 مار 2000 الخاص بالتوقيع الإلكتروني بأنه "دليل كتابي مؤلف من مجموعة من الحروف والأشكال أو الأرقام أو من الإشارات أو رموز لها مدلول أيا كانت الدعاية المثبتة بشرط أن يكون في الإسكان بالضرورة تعيين الشخص الذي صدرت منه وأن تعد وتحفظ في ظرف من طبيعتها ضمان سلامتها" خالد فهمي 44 .

أما قانون المعاملات والتجارة الإلكترونية لحكومة دبي لسنة 2000 فقد عرفته بأنه توقيع مكون من حروف أو أرقام أو رموز أو نظام معالجة في شكل إلكتروني ويلحق أو يرتبط برسالة إلكترونية وجمهور نية توثيق أو اعتماد تلك الرسائل.

أما المشرع الأردني فقد عرفه في القانون كالمؤقت رقم 2000/85 من قانون المعاملات الإلكترونية بأن البيانات التي تتخذ هيئة أو ظروف أو أرقام أو إرشادات أو

غيرها وتكون مدرجة بشكل إلكتروني أو رقمي أو ضوئي أو أي وسيلة أخرى مماثلة في رسالة معلومات أو مضافة عليها أو مرتبطة بها ولها طابع يسمح بتحديد هوية الشخص الذي وقعها ويميزه عن غيره من أجل توقيعه وبفرض الموافقة على مضمونه " عمر المؤمني 146.

وبدافع الضرورة قد خل المشرع الأوروبي لوضع تعريف بالتنسيق من الدول الأوروبية في مجال الإعتراف بالدليل الإلكتروني فأصدر التوجيه الأوروبي 13-12-1999 حول الإرشادات والتوجيهات في الإطار التشريعي المشترك للتوثيق الإلكتروني[386] حيث عرف أن بيان أو معلومة معالجة إلكترونيا يرتبط من خلال التقنيات المنظمة بالمعلومات الواردة في المحرر الإلكتروني ويتيح لصاحبه أن يعبر عن قوله بمضمون هذه المعلومات وإلتزامه بها ، ويشترط لهذا التوقيع أن يكون مرتبطا بشخص يصدره وأن يكون محددا بشخص وصدر التوقيع ومميزا له عن غيره من الأشخاص وأن يتم إنشاءه أو إصداره من خلال تقنيات وإجراءات تسمح مصدر التوقيع بالإستئثار به والسيطرة عليه على نحو موثوق به يكون مرتبطا بالمعلومات التي يتضمنها المحرر الإلكتروني وبطريقة تسمح بإكتشاف أي تعديل مادي في مضمون المحرر أو التوقيع أو الفصل بينهما[387] (خالد فهمي 44- 43).

أما المشرع المصري فعرفه في المادة 1/جـــ من قانون التوقيع الإلكتروني رقم 2000/15 الصادر في 2004/04/22 بأنه يوضع على محرر إلكتروني ويتخذ شكل حروف أو أرقام أو رموز أو إشارات أو غيرها ويكون له طابع متفرد يسمح بتحديد شخص الموقع بميزة عن غيره ممدوح مبروك 05-06.

أ/ التوقيع الإلكتروني في توجيهات الإتحاد الأوروبي

---

[386] Pour avoir plus: Éric CAPRIOLI, La directive européenne n° 1999/93/CE du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques, Revue Gazette du Palais, 31 octobre 2000 n° 305, P. 5

[387] **Sylvain MARTIN, Arnaud TESSALONIKOS, La signature électronique , premières réflexions après la publication de la directive du 13 décembre 1999 et de la loi du 13 mars 2000, Revue Gazette du Palais, 20 juillet 2000 n° 202, P. 4**

نجد في توجيهات الإتحاد الأوروبي نوعان من التوقيع الإلكتروني وهما :

التوقيع الإلكتروني : "معلومات على شكل إلكتروني متعلق بمعلومات إلكترونية أخرى ومرتبطة بها إرتباطا وثيقا ويستخدم أداة التوثيق" (نصيرات 24).

ب/ التوقيع الإلكتروني في القانون الأمريكي :

يوجد تعريفات للتوقيع الإلكتروني في القانون الأمريكي تعريف في القانون الفدرالي في المادة 08/102 بأن التوقيع الذي يصدر في شكل إلكتروني ويرتبط بسجل إلكتروني وتعريف ثاني ورد في قانون المعاملات الإلكترونية الموحد [388] وعرف بأنه (نصيرات 25).

"صوت أو رمز أو إجراء يقع في شكل إلكتروني يلحق (يرتبط منطقيا بعقد أو سجل آخر (وثيقة) ينفذ أو يصدر من شخص يقصد التوقيع على السجل " (نصيرات 25)

ويلاحظ على التعريفات ما يلي :

فتح المجال أمام أي وسيلة لم ينص عليها في التعريف تقع في شكل إلكتروني تكون قادرة على تحقيق متطلبات التوقيع الإلكتروني والإعتراف بها كوسيلة صالحة للتوقيع .

عدم اشتراط ارتباط التوقيع ارتباطا ماديا بالسجل الذي يقع عليه كما هو الحال في التوقيع الخطي الذي يلحق بالكتابة بل اكتفى بارتباطه ارتباطا منطقيا".

وسع من عملية تنفيذ أو إصدار التوقيع واعتمدها بأي طريقة كانت ولم تتطلب عملية التوقيع بخط السيد.

ج/ التوقيع الإلكتروني في القانون الفرنسي :

أما قانون المعاملات الإلكترونية الموحد فيلاحظ عليه :

---

[388] **Bruno P. LANGLOIS, La protection des marques sur internet : le législateur fédéral américain s'attaque à la cyberpiraterie, Revue Gazette du Palais, 20 juillet 2000 n° 202, P. 29**

لم يحدد صورا للتوقيع الإلكتروني بل اكتفى بان يكون التوقيع في شكل إلكتروني اعتقادا منه بأن هذا المنحى أجدى بالإعتراف بصور أخرى للتوقيع الإلكتروني التي تتمتع بالثقة الكافية ونحقق وظائف التوقيع.

- وجوب إرتباط التوقيع الإلكتروني بسجل إلكتروني وهذا الأخير يعرف بأنه أي عقد أو أي سجل آخر جرى إنشاءه أو رسالة أو استقالة أو تحريف بالوسائل الإلكترونية (نصيرات 26).

د/ التوقيع الإلكتروني في القانون المصري :

ورد تعريف التوقيع الإلكتروني في الفصل الأول من مشروع قانون التجارة الإلكترونية في مادته الأولى بأنه :

- التوقيع الإلكتروني حروف أو أرقام أو رموز أو إشارات لها طابع متفرد تسمح بتحديد بخص صاحب التوقيع ويميزه عن تميزه.

و من يلاحظ على هذا التعريف أنه :

حاول سرد جميع الأشكال التي يمكن أن يتكونه منها التوقيع الإلكتروني، إشتراط أن يكون مكونات التوقيع الإلكتروني ذات طابع متفرد حتى يضمن السرية التامة وتجنب إغتصاب التوقيع أو استجابة من قبل الغير وهذا الشرط يعني تحديد هوية الموقع وتميزه عن غيره وهي الوظيفة الأولى للتوقيع لم ينص عن الوظيفة الثانية للتوقيع وهي التعبير عن إرادة الموقع بالموافقة على مضمون الوثيقة أو السجل (نصيرات 28-29).

هـــ/ القانون الإلكتروني في القانون الأردني :

عرف المشرع الأردني التوقيع الإلكتروني في المادة 02 من قانون المعاملات أو أرقام أو رموز أو إشارات أو غيرها وتكون بدرجة شكل إلكتروني أو رقمي أو ضوئي أو أي وسيلة أخرى مماثلة في رسالة معلومات أو مضافة عليها أو مرتبطة بها ولها طابع يسمح بتحديد هوية الشخص الذي وقعها ويميزه عن غيره من أجل توقيعه وبغرض الموافقة على مضمونه.

وما يلاحظ على هذا التعريف ما يلي :

عدم حصر الطريقة التي يرد بها التوقيع بدلالة قوله "أو غيرها"

إشتراط التعريف أن تكون البيانات مدرجة بشكل إلكتروني ومضافة على رسالة البيانات.

إشتراط كذلك أن تكون تلك البيانات تسمح بتحديد هوية الشخص الذي وقع رسالة البيانات ومميزة له وكاشفة عن موافقته على مضمونها (نصيرات ، 29–30).

و/ التوقيع الإلكتروني في قواعد الأونسترال

يرجع إلى الإنترنت

02– تعريف التوقيع الإلكتروني في الفقه :

عرف البعض التوقيع الإلكتروني بأنه هو الذي يقوم على مجموعة من الإجراءات والوسائل التي تتيح استخدامها عن طريق الرموز أ, الأرقام إخراج رسالة إلكترونية تتضمن علاقة مميزة لصاحب الرسالة المنقوبلة إلكترونية يجري تشفيرها بإستخدام خوارزم المفاتيح واحد معلن والآخر خاص لصاحب الرسالة وعرف أيضا بأنه مجموعة من الإجراءات التقنية (نصيرات 30)التي تسمح بتحديد شخصية من تصدر عنه هذه الإجراءات وقبلوه بمضمون التصرف الذي يصدر التوقيع بمناسبته.(نصيرات 30)

وما يلاحظ على هذا التعريف :

- لم يورد شكلا ولا طريقة معينة لأنة تعد أو تعتبر تواقيعا إلكترونية .
- حصر التعريف وظائف التوقيع الإلكتروني التي يجب أن توفرها الإجراءات التقنية المعتمدة هي تحديد هوية الموقع أولا وثانيا التعبير عن إرادته بالموافقة على مضمون السند أو الوثيقة أو السجل الذي تم التوقيع عليه.
- يترك المجال واسعا للمشرع الوطني أن يكيف التفاصيل المتعلقة بالتوقيع الإلكتروني (نصيرات 31).

الفرع الثاني : شروط التوقيع الإلكتروني

وقد التزم التوجيه الأوروبي الدول الأعضاء بالإتحاد بمنح هذا التوقيع الحجية القانونية التي يتمتع بها التوقيع الخطي الكتابي وهو ما أعطى التوقيع الإلكتروني نفس درجة التوقيع الكتابي وهو ما اعتبره البعض دليلا كاملا في ألإثبات طالما توافرت فيه الشروط القانونية 389 وهذا من شأنه تشجيع نمو التجارة الإلكترونية وبقدر كفالة الحماية له تقرر حماية تابعة للتجارة الإلكترونية[390].

ولكي يعتمد التوقيع الإلكتروني بنفس الحجية القانونية التوقيع الكتابي اشترط فيه التوجيه الأوروبي السابق جملة شروط : (فيصل الغريب 220)

- أن يكون التوقيع مرتبطا بشخص يصدره.
- أن يكون محددا لشخصية الموقع مميزا له عن غيره.
- أن يكون مرتبطا بالمعلومات التي يتضمنها المستند الإلكتروني بطريقة تسمح بإكتشاف أي تعديل يطرأ عليه أو على المستند.

كما نص الفصل الثالث من قانون التجارة الإلكترونية المصري على منح التوقيع الإلكتروني الحجية المقررة للتوقيع الكتابي أو الخطي وإعتماده في الإثبات بشروط هي :

- إرتباط التوقيع الإلكتروني بالموقع دون غيره.
- سيطرة الموقع دون غيره على الوسيط الإلكتروني.
- إمكان كشف أي تعديل أو تبديل في بيانات المحرر الإلكتروني أو التوقيع الإلكتروني.

الفرع الثالث : عناصر التوقيع الإلكتروني

للتوقيع الإلكتروني وفي جملة خصائص يمكن عملها فيما يلي أنه :

---

[389] فيصل الغريب ، 220.

[390] **Éric CAPRIOLI, La directive européenne n° 1999/93/CE du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques, Revue Gazette du Palais, 31 octobre 2000 n° 305, P. 5 et**

Thierry PIETTE-COUDOL, LCEN. L'écrit électronique et la signature électronique depuis la LCEN, Revue Communication Commerce électronique n° 9, Septembre 2004, Etude 29

يتشكل من عناصر متفردة خاصة بالموقع (حروف ، رموز ، أرقام ، إشارات).

يحدد شخص الموقع ويبين هويته.

يعبر عن رضاء الموقع وإلتزامه بالتصرف القانوني الذي يحويه المحرر الإلكتروني يوضح على المحرر الإلكتروني ويتصل به غير وسيلة إلكترونية.(ممدوح مبروك ، 08).

الفرع الرابع : صور التوقيع الالكتروني:

أخذ التوقيع الالكتروني أشكالا متعددة في التعاملات التجارية، و هو يأخذ صور مختلفة عن بعضها الرابط بينها أنها تقوم على الوسائط الالكترونية، و استخدام التقنيات الحديثة التي تجعل الشخص يحتكر بعض الإجراءات التقنية لنفسه للتوقيع على بيانات أو وثائق أو عقود إلكترونية لما تنتجه تكنولوجيا المعلومات.

01- التوقيع الإلكتروني المعزز :

هو عبارة عن توقيع إلكتروني يشترط فيه أن يكون :

مرتبطا إرتباطا فريدا من نوعه مع صاحب التوقيع.

قادر على تحقيق (تحديد) صاحب التوقيع والتعرف عليه بإستخدامه.

تم إيجاده باستخدام وسائل يضمن فيها صاحبه السرية التامة. (نصيرات 24).

مرتبط مع المعلومات المحتواة في الرسالة حيث أنه يكشف أي تغيير في المعلومات

02- التوقيع الرقمي أو الكودي:

يستخدم هذا التوقيع في التعاملات البنكية و غيرها من التعاملات التجارية الإلكترونية و يعتبر من أهم صور التوقيع الإلكتروني و يعتبر لدى البعض الأفضل على الإطلاق لما يتمتع به من درجة عالية من الثقة و الأمان.

و التوقيع الرقمي هو ذلك التوقيع الذي جاء نتيجة الاستفادة من تطور علم التشفير فيتم إنتاجه باستخدام تقنيات هذا العلم، و هو اصطلاح يطلق على عملية تتضمن تشكيل و إنشاء رسالة الكترونية و تشفيرها (بأرقام و خانات رقمية) لتشكيل ما يعرف بالبصمة الالكترونية لترسل إلى طرف آخر يستوثق بعد فتحها من مضمونها و شخصية مرسلها و سلامة الرسالة من التعدي أو التزوير.

و تكنولوجيا التوقيع الرقمي يقدم بديلا و ظيفيفيا لتوقيع الخطي التقليدي.[391]

و أكثر استعمالاته أنه يعتمد على تقنية التشفير غير المتماثل الذي بدوره يرتكز على زوج من المفاتيح غير المتماثلة، المفتاح الأول يكون معروف للجميع و يحتفظ به سرا يسمى عام أما المفتاح الثاني يسمى مفتاح خاص بصاحبه و يحتفظ به سرا و يستطيع به تشفير رسالته[392].

خلاصة القول أن التوقيع الرقمي يتم من خلال معادلات رياضية باستخدام اللوغارتميات يتحول بها التوقيع أو المحرر المكتوب من نمط الكتابة العادية إلى معادلة رياضية لا يمكن لأحد أن يعيدها إلى الصيغة المقروءة إلا للشخص الذي لديه المعادلة الخاصة بذلك المفتاح العام و الخاص[393].

و يستهدف من استخدام التوقيع الرقمي في مجال التجارة الالكترونية أن يحقق ما يلي:

أ/ موثوقية الرسالة الالكترونية:

إن استخدام المفتاحين العام و الخاص من شأنه أن يحدد هوية الشخص الموقع بأمان بإمكانية التزوير أو الانتحال مستبعدة إلا بفقد المفتاح الخاص.

---

[391] - المؤمني 51

[392] - نصيرات 37-38.

[393] - نصيرات 38، للإطلاع أكثر على كيفية عمل التوقيع الرقمي أنظر مؤمني 54-70

فيحقق.....الرسالة الالكترونية من مصدرها الحقيقي و تحقيق طمأنينة للمستقبل لها.....394

ب/ توثيــق الرسالـــة:

تضمن التوقيع الرقمي المعتمد على المفتاحين العام و الخاص سلامة الرسالة بأي تزوير أو أي تغير فيها يكشفه التوقيع الرقمي من خلال معالجة النتائج المتحصل عليها من الدوال الرياضية التي تعمل عن التوقيع و الأخرى عند التوثيق، و تشخيصها395.

و هو ضمانة لكون الرسالة الالكترونية قد تلقاها المستقبل بنفس المحتوى التي أرسلها دون أن يتم تعديلها أو تفسيرها أو تزورها396.

ج/ تحديد صاحب التوقيع:

إن اعتماد التوقيع الإلكتروني على المفتاحين العام و الخاص، يعتبر في حد ذاته ضمانة لتحديد هوية الموقع إذ لا يمكن استخدامه من قبل شخص آخر إلا إذا فقد المعني به السيطرة عليه،

و التوقيع الرقمي يوفر طمأنينة للمستقبل بأن الرسالة التي تلقاها لا يمكن بأي حل أن ينشأها أو يرسلها إلا المرسل الحقيقي.

د/ سريـــة الرسالـــة:

ليجب أن تثبت لدى المرسل المستقبل كلاهما بأن الرسالة الإلكترونية المتبادلة بينهما و الموقعة بهذه الصورة لا يمكن _ لأي شخص غير مخول _ قراءتها أوالاطلاع على محتواها397.

هـــ/ الفعاليـــــة:

394 - مؤمني 52
395 - نصيرات 40
396 - مؤمني 32
397 - مؤمني 52

يعد التوقيع الرقمي من أهم صور التوقيع الالكتروني لما يوفره من..... خال من الضمان و السرعة و الدقة العالية و الأمان بالإضافة إلى أن احتمال وقوع العطل أو حدوث المشاكل الأمنية من غيره من احتمال التلاعب به أو تزويره[398].

03- التوقيع البيومتري:

يعتمد هذا النمط بين التوقيع على الصفات و الخواص الفيزيائية و الطبيعية و السلوكية للإنسان و التي تختلف بالضرورة من شخص لآخر[399].

و تتمثل آلية عمله أنه يتم باستعمال إحدى الخواص الذاتية للشخص (قزحية العين، بصمة الإصبع، بصمة الكف، بصمة الشفاه، نبرة الصوت) حيث تخزن بصورة رقمية مضغوطة في ذاكرة الكمبيوتر[400]، و ذلك بطريق التشفير للتحقيق من صحة التوقيع و ذلك بمطابقة صفات و سمات العميل المستخدم للتوقيع مع الصفات التي تم تخزينها على جهاز الحاسب الآلي[401].

و يتساءل البعض عن مدى الثقة التي توفرها هذه الصورة و التوقيع، فنجد أن الفقه قد اختلف في ذلك و الراجح في الآراء أن إمكانية تزويرها أو نسخها هي إلى الوقوع أقرب منها إلى العدم حيث يمكن لقراصنة الحاسب الآلي صناعة عدسات لاصقة، بنفس اللون و الشكل و الخصائص المخزنة على الحاسب أو تسجيل بصمة الأصبع أو نبرة الصوت عن طريق البصمات البلاستيكية[402].

بالرغم من إدعاء الشركات المصنعة أي بنسبة الأمان تصل 99 أو 100% [403]

كما أنه يقلل من مدى فعاليتها.... انطوائها على معدل خطأ يرتفع بمعدل ارتفاع عدد الأشخاص الذين تخزن خصائصهم لاحتمال وقوع الخطأ و الارتياب كما تتغير دقتها

---

[398] - نصيرات 40
[399] - الغريب 23
[400] - نصيرات 32
[401] - نجيبة أبو هيبة 50
[402] - أنظر في هامش نجوى أبو هيبة 51
[403] - ثروت عبد الحميد 61

بحدوث تغيرات طبيعية على الموقع ذاته على سبيل المثال تغير نبرة الصوت نتيجة مرض أو تناول أدوية أو تعرض أصابع اليد إلى حروق أو إصابتها بجروح بها يمنع المستخدم الشرعي من استخدام توقيعه404.

04- التوقيع بالقلم الالكتروني:

تتمثل طريقة التوقيع بالقلم الالكتروني في استخدام قلم الكتروني حساس وظيفته الكتابة على شاشة الحاسب الآلي عن طريق برنامج محرك لهذه العملية و يؤدي هذا البرنامج أو يقوم بوظيفتين:

خدمة التقاط التوقيع و خدمة التحقق من صحة المشفر405

الاستناد إلى حركة هذا القلم على الشاشة و الأشكال التي يتخذها من دوائر أو انحناءات أو إلتواءات أو نقاط و درجة الضغط على القلم و سمات أخرى ... للتوقيع الشخصي و التي يكون قد سبق تخزينها بالحاسب الآلي406 و فهمه التشفير هنا للحفاظ على أمن و سرية التوقيع407.

كما تستخدم في حفظ و تخزين المراسلات الالكترونية و المعاملات التجارية و يتلقى البرنامج أولا بيانات العمال عن طريق بطاقته الخاصة و يتبع بعد ذلك الشخص التعليمات التي تظهر في الشاشة و تظهر رسالة بعد ذلك مطالبة بتوقيعه باستخدام قلم على..... داخل الشاشة، و يقوم الشخص بالضغط على مفاتيح معينة تظهر له على شاشة بأنه موافق أو غير موافق على توقيعه 408، بعدها يأتي دور خدمة التحقق من صحة التوقيع و هي يقوم بفك التشفير و تقارن المعلومات: المقدمة مع التوقيع المخزن ليقرر الحاسب إذا ما هذا التوقيع صحيحا أم أنه غير مطابقة للمواصفات المخزنة

404 - الحكومة الالكترونية الهامش 176-177
405 - الغريب 231
406 - ممدوح مبروك 14-15
407 - المادة 30 من مشروع التجارة الالكترونية المصري، أبو هيبة نجوى، الهامش 52.
408 - مجازي ت إ ح ج 199

لديه409 إلا أن تداول هذه الطريقة تثير العديد من المشاكل أهمها إثبات الصلة بين التوقيع و المحرر المرسل حيث تفتقد التقنية التي يتم بها، لاستيثاق من قيام هذه الرابطة بالإضافة إلى إمكانية قيام المرسل إليه الإحتفاظ بنسخة من صورة التوقيع الفعلي، و من منطلق كون أن قوة الصلة بين التوقيع و رسالة البيانات تمثل جوهر الاعتراف لحجية التوقيع في الشكل الالكتروني410.

المطلب الثاني : الجرائم الواقعة على التوقيع الالكتروني:

إن اعتماد التوقيع الالكتروني الذي هو عبارة عن ملف رقمي معترف به من قبل المشروع يهدف إلى الحفاظ على مستوى من الثقة و الأمان بالنسبة للمتعاملين من ناحية قدرته على الحفاظ على سرية المعلومات أو الرسائل و تحديد هوية المرسل و المستقبل و كذا التأكد من صدق المعلومات.

و قبل ظهور القواعد القانونية.... المتعلقة بمعاملات التجارة الالكترونية لم تكن هناك قيمة قانونية للعقود الالكترونية و كذا التواقيع الالكترونية و لعل من بين المشرعين و الأوائل إلى كفالة تشريع قانوني ينظم و يعترف بهذه المعاملات هذا النمط من العقود هو المشرع الأوروبي[411] الذي حث في مبادرة له على إيجاد إطار قانوني ... بين الدول الأوروبية412، و بالنسبة لما يتعلق بالتوقيع الالكتروني فقد أصدر التوجيه الأوروبي رقم 1999/93 الصادر بتاريخ 13 ديسمبر 1999 في شأنه إطار أوروبي للتوقيع الالكتروني بعصيان تأخذ الشكل الالكتروني، ترتبط بعصابات أخرى الكترونية و تستخدم كوسيلة لإثبات صحتها 413، و تقرر بهذا التوجيه صحة التوقيع الالكتروني و

409 - هدى قشقوش، ح ج ت إ، 78
410 - ثروت عبد الحميد 55-56

411 Danièle VÉRET et Carole FONGUE, La signature électronique va-t-elle révolutionner le formalisme des marchés publics ?, Revue Gazette du Palais, 23 janvier 2001 n° 23, P. 9

412 - مدحت رمضان 27، مجدي 295.
413 - مجازي 295، مدحت لرمضان 27.

الاعتراف به و بالخدمات المرتبطة به[414] و بخصوص الحماية الجنائية المقررة للتوقيع الالكتروني.

الفرع الاول : الدخول بطريق الغش على قاعدة بيانات تتعلق بالتوقيع الالكتروني:

جاء النص على هذا الاعتداء في المادة 26 من المشروع المصري للتجارة الالكترونية مع عدم الإخلال بأية عقوبة أشد وردت في قانون آخر، يعاقب بالحبس و بغرامة لا تقل عن 300 جنيه أو باء حدى هاتين العقوبتين، كل من دخل بطريق الغش أو التدليس على نظام معلومات أو قاعدة بيانات تتعلق بالتوقيعات الالكترونية، و يعاقب بنفس العقوبة من اتصل أو أبقى الاتصال بنظام المعلومات أو قاعدة البيانات بصورة غير مشروعة415.

01- مفهوم بيانات التوقيع الالكتروني:

هي تلك المعلومات المتعلقة بصاحب التوقيع من اسمه، مهنته و معلومات شخصية و معلومات خاصة بذلك التوقيع و بياناته السرية، و إذا ما تمت معالجة هذه آلية وفق تغذية الكترونية حتى تصير برنامجا تصبيقا. يحمل للحاسب الآلي لتشغيل و تحصيل نتائج تخص التوقيع الالكتروني و هذا باسمي النظام المعلوماتي416.

02- الركـــن المـــادي للجريمة:

و الجريمة تقوم إذا ما تم الدخول إلى قاعدة البيانات أو النظام المعلوماتي الخاص بالتوقيع الالكتروني من قبل الجاني دون اشتراط تحقق نتيجة ما كأثر لذلك الدخول الذي

---

[414] **Éric CAPRIOLI, La directive européenne n° 1999/93/CE du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques, Revue Gazette du Palais, 31 octobre 2000 n° 305, P. 5**

[415] - هدى حامد قشقوش 48-49.
[416] - حجازي 296-297

تم بطريق الغش أو التدليس417 أي مجرد فن المشروعية أي بدونه إذن قضائي أو إذا لم يكن من أولئك الأشخاص الذين عقد لهم الاطلاع على ذلك النظام أو النظام أو قواعد بياناته كما يمكن أن بأنه الركن المادي لهذه الجريمة صورة أخرى إذا كان الجاني يملك صلاحية الاتصال بنظام المعلومات أو قاعدة بيانات التوقيع الالكتروني لكنه تجاوز الفترة المسموح له البقاء و الاتصال فيها و أبقى الاتصال قائما، أو أن يقوم ذات الشخص الجاني بالاتصال بالنظام أو قاعدة البيانات بغير وجه مشروع418.

03- الركــن المعنــوي للجريمة:

إذا كان الجاني يعلم أنه مقلد مخالف للقانون أو يشكل اعتداءا على حق غيره بوصف الفعل جرما و انصرفت إرادته إلى أداء الفعل و حدوث نتيجته عند سلوكه جرما مصحوبا بقصد جنائي، لا يتصور وقوع هذه الجريمة بطريق الخطأ لأنها من الجرائم العمدية و التي ركنها المعنوي بدوافع القصد الجنائي العام بعنصرية العلم و الإرادة.

الفرع الثاني : جريمة صنع أو حيازة برنامج لإعداد توقيع الالكتروني:

نصت المادة 27 من مشروع القانون المصري على أنه "يعاقب بالحبس مدة لا يقل عن سنة و بغرامة لا تقل عن عشرة آلاف جنيه أو بإحدى هاتين العقوبتين، كل من صنع أو حاز على نظام معلومات أو برنامج لإعداد توقيع الكتروني دون موافقة صاحبه"419

و محل الجريمة هذه صناعة توقيع الكتروني دون ترخيص و موافقة صاحبه بواسطة نظام أو برنامج معلوماتي و يشترط الفقه للعقاب على السلوك ما يلي420 و هي تتشكل عناصر الركن المادي.

01- الركن المادي :.....

أ/ صناعة برنامج أو نظام معلوماتي:

---

417 - حجازي 297.
418 - حجازي 297-298.
419 - هدى قشقوش 49.
420 - حجازي 299-300.

الجاني هذا الشرط يقوم بصناعة النظام أو إنشاء برنامج معلومات لأجل إعداد توقيع الكتروني، أي أن الجاني يخلقه من العدم و يصممه حسب المواصفات الفنية و التقنية التي يتوصل منها إلى إنتاج توقيع الكتروني، سواء أكان هذا الشخص الذي قام بصناعة النظام أو البرنامج لإعداد التوقيع شخصا طبيعيا أو شخصا اعتباريا و سواء كانوا مرخصا لهم بالعمل في هذا المجال أو غير مرخص لهم421.

ب/ عدم رضا أو علم صاحب التوقيع:

مناط التجريم في هذه الجريمة هو قبول صاحب التوقيع أو عدم موافقته حيث كلما تخلفت إرادة صاحب التوقيع وقع سلوك الفاعل تحت طائلة عدم المشروعية و لذلك فإن موافقة صاحب التوقيع هي التي تخرج من نطاق هذه الجريمة ما تقوم به الجهة المرخص لها حسب القانون بإعداد توقيع الكتروني للشخص طالما يتم ذلك برضاه و ليس رغما عن إرادته[422].

ج/ قدرة البرنامج أو النظام على صناعة توقيع الكتروني (أو إيجاده):

متى استطاع الجاني بواسطة هذا البرنامج الذي أنشأه أو هذا النظام الذي صممه إيجاد توقيع الكتروني أو إيجاده قام في حقه التجريم، و يسقط عنه الوصف الجرمي متى كان ذلك البرنامج أو النظام فاقدا للمقدرة الفنية لعمل توقيع الكتروني و لم يحقق له غرضه الإجرامي، كما يستوي كذلك أن يستخدم وسائل و أجهزة و أدوات يختلس بها معلومات عند توقيعات قائمة بالفعل يحصل على نسخة فيها دون موافقة أصحابها بصرف النظر عن تمام استخراج التوقيع من عدمه حيث العبرة بضاعة البرنامج أو النظام دون النظر إلى تمام الحصول على التوقيع أو عدمه423.

و صورة أخرى للركن المادي و هي حيازة برنامج أو نظام معلوماتي لاعداد توقيع الكتروني دون موافقة صاحبه، و معنى الحيازة غير المشروعة أي أن لا يكون الجاني مالكا له أو مستأجرا أياه أو مستعيرا له من آخر، يعني أنه من الأشخاص غير المرخص لهم بحيازة البرنامج أو النظام المتعلق بالتوقيع فالحيازة المشروعة لا عقاب

---

421 - حجازي 249-300.

422 **Philippe BOURE, Internet et la lutte contre la cybercriminalité, Revue Gazette du Palais, 23 janvier 2003 n° 23, P. 19**

423 - الحجازي 300.

عليها طالما أن الشخص مرخص له بها من الجهة الوصية و المختصة و هدف هذه الجهات المختصة من منح التراخيص للأشخاص (طبيعيين و اعتباريين) الراغبين في إعداد هذه البرامج أو صناعتها أو استيرادها هو توثيق هذه التوقيعات ففي حالة عدم وجود هذه التراخيص أو ثبوت اتجاه نية من يمتلك مثل هذا الترخيص إلى استخراج توقيع دون موافقة صاحبه و رغما عن إرادته قامت الجريمة بركنها المادي دون النظر لتمام التوقيع الالكتروني من عدمه424.

02- الركـــن المعنـــوي:

إذا علم الجاني بأن كافة الوقائع المكونة لسلوكه الإجرامي تشكل مخالفة للقانون و إذا انصؤفت مع ذلك إرادته إلى إحداث الفعل الإجرامي مع قبول ما يترتب عنه من نتائج تحكم بأن عنصري العلم و الإرادة المشكلان للقصد الجنائي العام قد توافر و بذلك قام الركن المعنوي لهذه الجريمة425.

ويرى الفقه أن هذه الجرائم تعد من جرائم السلوك المجرد أو جرائم الخطر حيث لا يشترط للعقاب عليها ضرورة حصول نتيجة إجرامية ما 426 و لا يعلق المشرع تجريم السلوك على حدوث أيما نتيجة كالجريمة التي سبقتها أي جريمة دخول بطريق الغش كما أسلفنا.

كما أنه لا عقاب على الشروع فيها بل اشترط المشرع تمام حدوث الفعل أي صناعة برنامج أو نظام معلوماتي لعمل توقيع الكتروني، كما أنه لا عقاب على الأعمال التحضيرية و هذا واضح من صياغة نصوص التشريع التي وردت بـــ مصطلح "صنع" أي أنجز الفعل و أتمه فضلا عن كون هذه الواقعة جنحة و لا عقاب على الشروع في الجنح427.

و يعني ذلك أن مثل هذه الجرائم هي من جرائم السلوك المجرد التي لا تفترض تحقق نتيجة من أي نوع، و لعل العلة في ذلك هو حماية الحق في السرية الذي يشكل اتصال الجاني غير المشروع بنظامه مساسا بالحق ذاته.428

الفرع الثالث : جريمة تزوير التوقيع الالكتروني:

---

424 - حجازي 301.
425 - حجازي 303.
426 - حجازي 301.
427 - حجازي 301.
428 - شمس الدين 145-146.

نصت المادة 28 من قانون التجارة الالكترونية المصري على أنه "مع عدم الإخلال بأية عقوبة أشد وردت في قانون آخر، يعاقب بالحبس مع الشغل كل من زور أو قلد محررا أو توقيعا الكترونيا أو شهادة اعتماد توقيع الكتروني مع علمه بذلك"

استهدف المشرعون في كافة الدول من تجريم فعل تزوير التوقيع الالكتروني حماية الثقة العامة للتوقيع، حيث يشكل الاعتداء على هذا التوقيع إهدارا أو إضعاف الثقة العامة للمتعاملين به حيث عامل الثقة أو الموثوقية تشكل ركيزة أساسية في النظام التجاري المرتكز على السرعة و الائتمان، و ليس صافيا من كون أن الإخلال بهذه الثقة هو إخلال بالضمان و اليقين و الاستقرار في المعاملات التجارية الالكترونية 429 و إن كان التزوير هو أخطر و أوسع استعمالا في مجال المعلوماتية أو سنعرض لبيانه باستقلالية.

01- الركن المادي :

أما بخصوص التوقيع الالكتروني فإن جريمة التزوير تأخذ صور في ركنها المادي إلا أنه يرتكز على فعل التقليد المعلوماتي واستعماله.

إذا التزوير الالكتروني يعني كل تغيير للحقيقة يرد على بيانات مخرجات سواء أكانت مخرجات ورقية أو مخرجات الكترونية.

و قد كان التشريع الفرنسي أكثر استيعابا في تعريفه للتزوير ..... حيث أدرج في التعريف حالتي الغش المعلوماتي الواقع على وثيقة معلوماتية حيث المادة 441 تستوعب التزوير العادي في المحررات بجانب تزوير الوثيقة المعلوماتية بصفة في لفظ سند أو دعامة و بأي وسيلة أخرى حيث لم يحصر وسيلة معينة يحدث بها الفعل430 .

يتحقق الركن المادي في هذه الجريمة بالتقليد أي تقليد توقيع الكتروني و يلحق به تزوير شهادة التصديق المنشأة للتوقيع حيث تعتبر شهادة التصديق ذات قيمة عالية ما يترتب عليها من آثار قانونية تتمثل في إنشاء التزامات و إثبات حقوقه بالنسبة لطرفي العلاقة التعاقدية التجارية الالكترونية و يلحق به نفس الوصف الإجرامي.

و الصورة الأخرى التي أجريت كذلك هي جريمة استعمال التوقيع الالكتروني المزور أو المقلد و كذلك شهادة اعتماد التوقيع الالكتروني المزورة. في ما إذا زورت أو قلدت

---

429 - تعرف الوثيقة المعلوماتية أو المعالجة معلوماتيا بأنها كل جسم منفصل أو يمكن فصله عن نظام المعالجة آليا للمعلومات، و قد سجلت عليه معلومات معينة سواءا أكان معدا للاستخدام بواسطة نظام المعالجة أو مشتقا من هذا النوع، حجازي، الدليل الجنائي، 149. حسام تمام 387.

430 - بسام تمام + نص المادة الفرنسي 403 الركن المادي.

لأجله، حيث جريمة الاستعمال مستقلة عن جريمة التزوير و الاستعمال يعني أو يقضي بإبرازه و الاحتجاج به فيما زور لأجله على اعتبار أنه صحيح 431 و أركان هذه الجريمة ثلاثة: نقل الاستعمال و محل يقع عليه هذا الفعل بالإضافة إلى القصد الجنائي432.

02- الركـــن المعنـــوي:

كلا صورتي جريمة التزوير أي التقليد أو الاستعمال هما من جرائم العمدية التي تقوم بالقصد الجنائي العام بعنصرين العلم و الإرادة. أي أنه يعلم الجاني أن فعله هذا يشكل مخالفة للقانون تتجرأ إرادته إلى إحداث نتيجته433.

نشر إلى أن في الإمارات العربية قانون إشارة دبي الخاص بالمعاملات و التجارة الالكترونية رقم 2 لسنة 2002 و في الفصل الرابع الخاص بالسجلات و التوقيعات الالكترونية المحمية ميزتين التوقيع الالكتروني و التوقيع الالكتروني المحمي بغرض تدعيم حماية التوقيع الالكتروني.434

الفرع الرابع : جريمة فض مفاتيح التشفير الالكتروني:

تطرق لهذه الجريمة المشرع التونسي في القانون الخاص بالمبادلات التجارية الالكترونية رقم 83 بند 2000 الصادر بـــ 09 أوت 2000 في المادة 48 حيث نصت على أنه "يعاقب كل من استعمل بصفة غير مشروعة عناصر تشفير شخصية متعلقة بإمضاء غيره بالسجن لمدة تتراوح بين 06 أشهر و عامين و بخطية تتراوح بين 1000 و 10.000دينار أو بإحدى هاتين العقوبتين"

و التشفير هو "تغيير في شكل البيانات عن طريق تحويلها إلى رموز أو إشارات لحماية هذه البيانات من إطلاع الغير عليها أو من تعديلها وتغيرها"435

التشفير يسمح بتلافي بعض المخاطر المتوقعة في استخدام تقنية المعلوماتية في المعاملات التجارية و قد كان مقتصرا في فرنسا على المجالات العسكرية و الدبلوماسية و الحكومية إلى غاية 1990 حيث سمح المشرع للمشروعات 19 الخاصة باستخدام

---

431 - إذا لم يقدم التوقيع ليتداول لا يمكن الإدعاء بوجوده، فجريمة الاستعمال لا تقوم سواء كان التوقيع موجود أو غير موجود فإن عدم من باب أولى لا تقوم. و إن وجد لا تقوم إلا بإظهاره.

432 - حجازي 306.

433 - حجازي 310

434 - نص المادة 19-20-21

435 - حجازي 311.

التشفير، ثم صور القرار رقم 98/101 بتاريخ 1998/02/24 الذي خفف من القيود المتعلقة بالتشفير و حدد الضوابط المتعلقة باستخدامه436.

و قد اجتهد المشرع في إسباغ حماية جنائية على البيانات المشفرة المودع شفرتها لدى مكتب التشفير و يخرج من نطاق هذه الحماية تلك المعلومات المشفرة التي كشفت نتائجها أو نصت شفرتها دون أن تكون مودعة لدى مكتب التشفير أي الجهة الخاضعة في تشفيرها لمكتب التشفير437.

و كشف مفاتيح الشفرة يكون بتسليم برنامج الشفرة أو فكها باستخدام تقنيات فنية متخصصة لمن ليس له حق في ذلك.

و يتم تشفير التوقيع الالكتروني بنظامين 438: الأول هو النظام السيمتري و هو عبارة عن برامج معتمدة على الرموز الهندسية المعقدة.

و الثاني النظام البيومتري و هو يعتمد على مواصفات شخصية متعلقة بصاحب التوقيع ذاته439.

الجريمة تقوم بمجرد تسليم مفاتيح فض الشفرة حتى و لو لم يستعملها من تسلمها تكون خطر استخدامها لا يزال قائم.

وفض شفرة التوقيع يعني إعلانها و إذاعتها و يعاقب عليها في حالة تسليمها لغير ذوي الشأن فإن سلمت بناءا على إذن قضائي أو إذن لإحدى الجهات المرخص لها قانونا كالبنوك مثلا.

و تجريم فض شفرة التوقيع الالكتروني يخدم مصلحة التجارة الالكترونية كون سرية التوقيع الالكتروني440.

و هذا الفعل يشكل الركن المادي لجريمة فض مفاتيح تشفير التوقيع الالكتروني أي ينقل التوقيع من صورة مكتوبة إلى صورة رقمية أي من صورة ذات دلالة معينة و مضمون معين ليكون مجرد إشارة أو رمز.

و المشرع التونسي اعتبر هذه الجريمة من جرائم السلوك المجرد حيث لم يتطلب تحقيق نتيجة معينة حيث تقوم الجريمة بمجرد فض الشفرة دون انتظار حصول ضرر للمجني عليه و هي بذلك تصنف ضمن جرائم الخطر و ليس جرائم الضرر.

---

436 - مدحت رمضان 32.
437 - حجازي 312.
438 - حجازي 312.
439 - أنظر في ذلك نصيرات .
440 - حجازي 313.

أما ركنها المعنوي فنحكم أنها من الجرائم العمدية فإنه يتطلب توافر القصد الجنائي العام أي أن يعلم الجاني بأن كل أفعاله تقع تحت طائلة عدم المشروعية و المخالفة للقانون و مع ذلك تتصرف إرادته إلى القيام بالفعل الإجرامي.

و العقوبة المقررة: عاقب المشرع التونسي بالحبس على هذه الجريمة من 06 أشهر إلى عامين و كذلك الغرامة من ألف و عشرة آلاف دينار مع ترك السلطة التقديرية للقاضي للجمع بين الحبس و الغرامة أو الإفراد.

المبحث الثالث : جرائم تزوير المحررات الالكترونية

لمعرفة شكل الحماية التي يمكن تقريرها ضد جريمة تزوير محررات التجارة الالكترونية يمكن أنه من الضروري الوقوف على علة تجريم هذا السلوك بعد تعريفه، فالتزوير هو: "تغيير الحقيقة بقصد الغش في محرر بإحدى الطرق التي نص عليها القانون تفسيرا من شأنه أن يسبب ضررا".[441]

و أما علـــة التجريـــم:

سبق و أن رأينا أن النشاط التجاري أيا كان صور تعاملاته مرتكز على ركنا السرعة و الائتمان، و إن وفرت تقنية المعلوماتية الركيزة الأولى و بطفرة ما كان لها نظير، ألا أنها ربما بقدر ما سهل المبادلات التجارية (أي المعلوماتية) بقدر ما شكلت تهديدا خطرا لنفس المبادلات بتهديدها لركن الائتمان حيث الباعث عليه هو ثقة المتعاملين بالتجارة الالكترونية و مداها، فأخطر ما شكل تهديدا لهذه المبادلات جريمة تزوير

[441] - جسام أحمد حسام طه تمام ، مرجع سابق ، ص 387.

المحررات الخاصة بهذه المبادلات الالكترونية [442] فخاصية المجرم المعلوماتي ..... على مدى قدرة ذكاءه، حيث ترتفع لدى الصنف من الجرم نسبة الذكاء المنبعث عادة من تحدي يعلن المجرم ضد النظم و البرامج المعلوماتية لقدرته على تخطي حاجز الأمان لأجل إثبات الذات و الكفاءة فقط هذا عموما و يكون الأمر أشد خطورة حينما يكون من جراء هذا الفعل مردود مادي لصالحه أو مقابل مغري من قبل الغير، خطورة هذا النوع من الإجرام تأخذ العديد من الصور و لعل أخطرها فعل التزوير و استعمال المزور.

و لذلك استهدف المشرع من تجريم فعل تزوير محررات المبادلات التجارية الالكترونية هو حماية الثقة العامة التي من شأنه الاعتداء عليها وقوع إحلال بالضمان و اليقين و الاستقرار في سائر نواحي معاملات التجارة الالكترونية.

و لعل أهم تساؤل يطرح بشأن مسألة ..... هي: هل تدرج المحررات الالكترونية محررات في مفهوم جريمة التزوير و تقع بها و تطبق عليها القواعد العامة الجزائرية أم يتعين استحداث نصوص تجرمه خاصة يزور محررات التجارة الالكترونية لتقرير حمايتها؟

المطلب الأول : موقـــف التشريـــعات مـــن جريـــمة التزويـــر المعلوماتـــي:

عموما خصص المشرع الفرنسي النص على جريمة تزوير المحررات المعرفية المادة 1/441 بقوله يعتبر تزويرا كل تغيير تدليس للحقيقة، يكون من طبيعته أن يسبب ضررا و يتم بأي وسيلة مهما كانت، في محرر أو سند للتعبير عن الرأي و الذي يكون موضوعه أو الذي من الممكن أن يكون له أثر في إنشاء دليل على حق أو فعل تكون له نتائج قانونية[443].

التزوير و استخدام المزور يعاقب عليها بالسجن ثلاث سنوات و 300.000 فرنك غرامة.[444]

الفرع الأول : الركـــن المـــادي:

---

[442] - ضبطت في الولايات المتحدة الأمريكية أكثر من 3 ملايين وثيقة مزورة تم تزويرها من قبل عصابة واحدة فقط، بلغت القيمة السوقية لما تم ضبطه 140 مليون دولار، أما في ولاية بنسلفانيا وحدها بلغت خسائر الشبكات الالكترونية المزورة 10 مليارات دولا سنويا، باسم الفقير 47- 48.

[443] **Nicolas MATHEY, Le commerce électronique dans la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, Contrats Concurrence Consommation n° 10, Octobre 2004, Etude 13**

[444] - حسام أحمد حسام طه تمام ، مرجع سابق ، ص 402- 403.

واضح من النص أن المشرع الفرنسي تطلب لقيام هذه الجريمة حدوث تغيير الحقيقة بأي وسيلة كانت و في هذا اللفظ دلالة على أن المشرع الفرنسي استبق فعل الإجرام المعلوماتي بأن عمم الحكم باختلاف وسائل ارتكاب الفعل ما كان معروفا منها و ما يمكن أن يستحدث و يكون محل جدل، و في هذا الاتجاه الذي توجهه المشرع الفرنسي اجتهاد تشريعي من شأنه أن يحد من درجة خطورة التزوير المعلوماتي لاشتمال النص على فعل التزوير (المعلوماتي) الالكتروني و قد نحى المشرع الجزائري بعض منحاه مع اشتراط حدوث الضرر و يستعرض صور هذا الركن عند ثلاث مشرعين.[445]

و قوام هذا الركن عند المشرع المصري هو وقوعه بطريق "الاصطناع أو التعديل أو التحويل أو بأي طريق آخر" بينما المشرع الفرنسي فقد اعتبر التزوير هو كل تغيير بطريق الغش في الحقيقة و من شأنه إحداث ضرر و يرتكب بأي طريقة كانت، أما المشرع الألماني فحص ثلاث صورا يقع بها هذا الركن في تزوير المستند الالكتروني أو لها إنشاء كل مصطنع و ثانيها قيام الجاني بتغيير الحقيقة فيه، ثالثها قيام الجاني بإحداث تأثير محل هذا السجل و هذا التحديد هو أكثر توفيقا من سابقيه حيث لم يفلح المشرع المصري في النص على التزوير لكون أن تغير الحقيقة له صور متعددة لم يستطع هو حصر هذه الطرق و هو أمر ..... ممكن.

و لما استشعر المشرع المصري عدم قدرته على هذا الحصر أردف عبارة " أو بأي طريق آخر"[446]

أما المشرع الفرنسي فقد رأى البعض أن نصه هو إلى الوصف أقرب منه إلى تحديد الفعل الذي تقوم جريمة التزوير، حيث في الحالة التي يقوم فيها الجاني باصطناع المستند لا يقوم فيها فعل تغيير الحقيقة في مستند قائم فقد لا يكون للمستند المصطنع من قبل الجاني نظر و الأصوب أن يعبر بالقول أنه " بيان غير صحيح " كيفما كان سبيل تحققه[447].

و حتى قبل تدخل **المشرع الفرنسي** انتهى القضاء في فرنسا إلى توافر صفة المحرر في الكتابة الالكترونية حيث قضت محكمة جنح باريس يتوافر وصف التزوير في

---

[445] - شمس الدين توفيق ، مرجع سابق ، ص 112- 113.

[446] - شمس الدين توفيق ، مرجع سابق ، ص 112.

[447] - شمس الدين توفيق ، مرجع سابق ، ص 113. **Agathe LEPAGE, Libertés sur l'Internet et cybercriminalité : les apports au droit pénal de la loi pour la confiance dans l'économie numérique du 21 juin 2004, Revue Droit pénal n° 12, Décembre 2004, Etude 18**

..... تزوير المحرر الالكتروني، بعد أن بحث مدى القوة القانونية لهذا المحرر و اعتد به في الإثبات و عليه أضفت المحكمة على الكتابة الالكترونية وصف المحرر في مفهوم جريمة التزوير.[448]

أمـــا سويـــرا: قد قضت المحاكمة الفدرالية السويسرية بتطبيق القواعد العامة في التزوير على الكتابة الالكترونية و نص بذلك القضاء الياباني لقبوله بفكرة التزوير في المحررات الالكترونية _ ما دام أن تلك المحررات يمكن قراءتها و نسبتها إلى صاحبها[449] و قد عدل المشرع السويسري مفهوم المحرر سويسرا ليشمل المحررات الالكترونية في قانون 1995 على أن الكتابة على دعامة للبيانات و دعامات الصور تعتبر في حكم المحررات.[450]

أمـــا بريطانيـــا: كما صدر في الحكمة المتحدة البريطانية قانون التزوير و التزييف لسنة 1981 عرف فيه المحرر في المادة 8–1 فيه بأنه يشمل " كل دسك أو شريط ممغنط أو صوتي أو أو كل وسيلة توجد بها أو عليها بيانات مسجلة أو محفوظة بطريقة ميكانيكية أو الكترونية أو بأي وسيلة أخرى"[451]

و هذا النص هو صريح في الاعتداء بالمحرر الالكتروني و مسايرة في ذلك القضاء الانجليزي حين قضت بوقوع جريمة التزوير في المحررات الالكترونية المعتمدة في البنوك و الشركات و قد توسع مع ذلك _ على خلاف الأنظمة اللاتينية _ في ..... بمفهوم التزوير حيث شمل تلك النصوص التي تحمي حقوق المؤلف، بذلك عندما أدمج في جرائم التزوير كل تقليد للبرامج الالكترونية و بيعها و طرحها للتداول التجاري على أساس أنها صحيحة و قضى تطبيقا لذلك سنة 1991 بوقوع جريمة التزوير في حق من قام بتقليد برامج الكمبيوتر و نسخها على دعامة و بيعها للمستهلكين على أساس أنها أصلية.[452]

التشريـــع الكنـــدي:

حرص المشرع الكندي على إدخال بيانات الكمبيوتر ضمن طائفة المحررات فيما يتعلق بجريمة تزوير المحررات دون النظر إلى المادة التي سجل عليها تلك البيانات إما على

---

[448] - TGI Paris. 12 Oct 1988, Lamy. DVR 1989. P24.شيماء عبد الغني ، مرجع سابق ، ص عبد الغني 83.

[449] - نحى هذا النحو القضاء اليوناني فيما قضت به المحكمة العليا في اليونان سنة 1983 لسيران وصف التزوير على المحررات الالكترونية، و قضت المحكمة العليا في هولندا سنة 1991 بنفس الاتجاه، شيماء عبد الغني ، مرجع سابق ، ص عبد الغني 84.

[450] - شيماء عبد الغني ، مرجع سابق ، ص 84.

[451] - شيماء عبد الغني ، مرجع سابق ، ص 85.

[452] - Affaire citée par David I.BAIN BRIDGE. Introduction to computer Law, London, Putman Publishing, 1993, P186، شيماء عبد الغني ، مرجع سابق ، ص عبد الغني 86.

الورق أو دعامة مادية أو في نظام الكتروني و نص في قانون العقوبات في المادة 321 منه على أن " المحرر يعني أوراقا أو أي مادة أخرى سجل أو مدون عليها ما يمكن قراءته أو فهمه من جانب الأشخاص أو أجهزة الكمبيوتر أو أي جهاز آخر، و يتضح من هذا النص صراحة اعتداد المشرع الكندي بالمحرر الالكتروني.[453]

التشريـــع الأسترالـــي:

عاقب القانون الأسترالي المعدل سنة 1983 في الفصل 276 بالحبس مدة لا تزيد على ثلاث سنوات كل شخص يقوم بتغيير أو تزوير أو مسح أو إتلاف أية بيانات مبرمجة بسوء نية.[454]

التشريـــع اليونانـــي:

وسع المشرع مفهوم المحرر و اعتبر المعلومات المبرمجة من قبيل المحررات في مفهوم جريمة التزوير و نص على أن المحرر يشمل كل وسيلة مستخدمة من جهاز كمبيوتر أو دعامة خارجية لتسجيل بيانات أو تخزينها أو نسخها بوسيلة الكترونية أو مغنطيسية تحتوي على معلومات أو صور أو رموز أو صوت في قانون 1988.[455]

و قضت المحكمة العليا في اليونان سنة 1983 بسريان وصف التزوير على المحررات الالكترونية.[456]

المطلب الثاني : طبيعـــة جريمـــة التزويـــر فـــي المحـــررات الالكترونيـــة:

نص المشرع الجزائري على جرائم التزوير في الفصل السابع من قانون العقوبـــــــات – دون أن يعرف جريمة تزوير المحررات –

و وزعها على أقسام ثمانية شملتها المواد 197 إلى 253 مكرر، لكن نرى أن أقرب هذه المواد شمولا للمحررات الالكترونية هي المادة 198 – في نظرنا – حيث عاقب على فعل الإصدار أو التوزيع أو البيع أو..... لأي من النقود أو السندات أو الأذونات أو الأسهم و التي هي في مجال التجارة الالكترونية تبعا لتطور التكنولوجي هي من قبيل المحررات الالكترونية..... اعتبار للوسيلة التي تم بها فعل التزوي ر. و الملاحظ أن درجة العقوبات المقررة يختلف حسب درجة خطورة الفعل الإجرامي و تراوحت ما بين الحبس و الغرامة إلى السجن المؤبد لكن كان من الأجدر إفراد

---

[453] - شيماء عبد الغني ، مرجع سابق ، ص عبد الغني 87.
[454] - شيماء عبد الغني ، مرجع سابق ، ص عبد الغني 87.
[455] - شيماء عبد الغني ، مرجع سابق ، ص عبد الغني 87.
[456] - شيماء عبد الغني ، مرجع سابق ، ص عبد الغني 84.

المحررات الالكترونية بنصوص خاصة بها لكثرة تداولها مستقبلا و اعتمادها في المجالات العمومية و التجارية على وجه الخصوص و لأجل حماية و كفالة الثقة لهذه المحررات باعتبارها وسيلة لا عن عنها لاثبات الحقوق و المراكز القانونية، و فصلا لأي نزاع مستقبلي بخصوصها على غرار بعض المشرعين في الدول العربية و الغربية.

صـــور التزويـــر:

و التزوير يتخذ صورا في المحررات الالكترونية

أولـــها: التلاعب في معلومات المحرر داخل النظام المعلوماتي بالتعديل للبيانات أو محرص فيما يغير من حقيقتها.

و الثانية: تتمثل في إدخال بيانات غير صحيحة لإنشاء محرر غير مطابق للحقيقة و تتم الصورتان بنية استعمال المحرر فيما زور لأجله فيما يراه البعض.[457]

المطلب الثالث : أركـــان جريمة تزوير المحررات الالكترونية:

لم يتطرق المشرع الجزائري لتعريف التزوير نستطيع بفضله بيان ماهية استيضاح أركان بل اقتصر على ذكر طرق وقوعه و المحتويات المقررة له مما جعلنا نتعرض لتعريفه من الفقه، حيث عرفه الفقه الفرنسي بأنه " تغيير الحقيقة بقصد الغش في محرر بإحدى الطرق التي نص عليها القانون تغييرا من شأنه أن يسبب ضررا "[458]

و عرفه الفقه المصري بأنه " تغير الحقيقة بإحدى الطرق المقررة بالقانون بقصد الغش في محرر صالح للإثبات و يرتب عليه القانون أثرا "[459]

يمكن أن نعرف المحرر أو نقصد به كل مسطور مكتوب، متضمن لعلاقات تعطى معنى معلوم و مترابط، دون اشتراط لغة في كتابة المحرر، و اشترط البعض في الكتابة أن تكون مركبة من حروف و إن لم تكن من نوع معروف كالكتابة المختزلة أو الشفرة السرية، دون النظر إلى المادة التي سطرت عليها الكتابة (ورق أو أقراص...)[460]

و عرف عند البعض بأنه المحرر المقصود في جريمة التزوير هو كتابة أحدهما بشخص (طبيعيا أو معنويا) من شأنها أن تولد مركزا قانونيا معينا أو ترتب نتائج معينة، شروط المحرر هي:

---

457 - السقا ، مرجع سابق ، ص 47.

458 - حسام أحمد حسام طه تمام ، مرجع سابق ، ص 386- 387.

459 - السقا ، مرجع سابق ، ص 48.

460 - حسام أحمد حسام طه تمام ، مرجع سابق ، ص 390- 391.

شرط الكتابة، شرط توافر خصائص معينة في الكتابة (السلامة، الثبات، الاستمرارية)، إمكانية حمل توقيع.[461]

و إذ لم تضع التشريعات نصوصا تحدد بموجبها المحرر الالكتروني و تحدد قوته و إذ لم تضع التشريعات نصوصا تحدد بموجبها المحرر الالكتروني و تحدد قوته في الإثبات و النصوص العقابية المتعلقة بالمساس به فإن الجدل لم ينتهي على مستوى الفقه بالأخص حول مدى جواز سريان النصوص العقابية التي تحمي المحررات الورقية على المحرر الالكتروني.[462]

فأخذ البعض بالتفسير الموسع لفكرة المحرر فذهب إلى اعتبار إمكانية أن يشمل المحرر الورقي و الالكتروني بالمعنى اللغوي لكلمة محرر أو مستند لا يقتصر على نوع معين من الكتابة، بل يشمل الكتابة على الورق كما ليتسع لغيرها من الصور و منها الكتابة الالكترونية أي يمكن أن يعتد بالكتابة على دعامة مادية غير ورقية أو غير مادية كأجهزة الحاسب الآلي و غيرها من نظم المعلومات[463] و رأى أصحاب هذا المذهب أن الشارع طالما لم يتطلب شكلا معينا من الكتابة أو مادة المحرر فيستوي أن تكون الكتابة بالمداد أو بالقلم أو الآلة الكترونيا مادام أن غاية ما يتطلب المشرع هو ثبوت نسبة المستند إلى صاحبه.[464]

أما الفريق الذي نادى بتطبيق التعريف و أخذ بالتفسير الضيق لمدلول المحرر فقد استند إلى كون أن النصوص العامة وظفت لتنظيم ما يتعلق بالمحر الوؤقي إذ لا يمكن سحب هذه النصوص على المحرر الالكتروني و يرون بجانب ذلك ضرورة أن يصدر المشرع تنظيما تشريعيا خاصا بالمحرر الالكتروني راعى فيها الضمانات التي يجب أن تتوفر في هذا المحرر هي تكفل له الحماية في مجال تعاملاته و يؤكد له أيضا فعالية و قبولا في المبادلات التجارية الالكترونية.[465]

و عرفه أيضا الفقه الفرنسي بأنه " تغيير الحقيقة في وقائع أعد المحرر لإثباتها متى كان من شأنه أن يسبب أضرارا و ارتكب بقصد الغش "[466]

و شأن جريمة التزوير كأي جريمة أخرى ترتكز على ركنان مادي و معنوي.

---

461 - شيماء عبد الغني ، مرجع سابق ، ص عبد الغني 80.
462 - شمس الدين توفيق ، مرجع سابق ، ص 22- 23.
463 - ثروت عبد الحميد 14.
464 - شمس الدين توفيق ، مرجع سابق ، ص 24.
465 - شمس الدين توفيق ، مرجع سابق ، ص 26.
466 - نجوى أبو هيبة 03.

الفرع الاول : الركـــن المـــادي:

و يتحقق هذا الركن و يقوم على عدة عناصر هي: تغيير الحقيقة و أن يقع على المحرر بالطرق التي حددها المشرع، و أن يحدث هذا التغير ضررا للغير.

و سنعرضها تبعا:

01- تغييـــر الحقيقـــة:

لتغيير الحقيقة أهمية قانونية، مستمدة من علة التجريم، و إن كان فعل التغيير ضروريا في جريمة التزوير إلا أنه لا يلزم أن تكون كل بيانات المحرر مغايرة للحقيقة، فيكفي أن يكون التغيير جزئيا أو نسبيا، بل يكفي لقيام هذه الجريمة أن يكون كل هذه البيانات أو بعضها مكذوبا بما يتعين على إثره أن يمس تغيير الحقيقة المركز القانوني للغير دون رضائه.[467]

و التغيير في جوهره نوع من الكذب يقع على المحررات يفترض لقيا م تدوين بيانات مخالفة للحقيقة.[468]

و التغيير في الحقيقة يكفي أن يقع على جزء من المحرر و ليس كله ذلك أن هذا التغير و إن قل أو صغر متعلق بإهدار الثقة، حيث إهدار الثقة في جزء من المحرر تكفي لإهدارها

في المحرر بأكمله و هو مجزء عن الكل ليتعدد به في القانون لقيام الجريمة.[469]

و لا يشترط لتحقق التزوير المعاقب عليه أن يكون فعل التغيير قد تم خفية أو أن يكون كشفه مما يستلزم جهدا و دراية خاصة فالعبرة بفعل التغيير دون الاعتداد بتقنيته فكونه واضح أو تطلب جهدا لكشفه نسيان مادام أن هذا التغيير في كلا الحالين ينخدع به الغير و يمس مركزا قانونيا.[470]

ثم إن مدلول تغير الحقيقة هو خاص فلا يشمل كل حالات الكذب المكتوب بل ينصرف فقط إلى التغيير الذي يمس حقا أو مركزا قانونا للغير، فإذا ما كانت البيانات الكاذبة لا تمس سوى مركز محرر المحرر هو نفسه تخلف النشاط الإجرامي هنا و يرد على ذلك استثناء في مثل هذه الإقرارات الفردية التي يتضمنها محرر رسمي و هي التي يكون

---

[467] - حسام أحمد حسام طه تمام ، مرجع سابق ، ص 388.

[468] - السقا ، مرجع سابق ، ص 50.

[469] - حسام أحمد حسام طه تمام ، مرجع سابق ، ص 389.

[470]- السقا ، مرجع سابق ، ص 50.

فيها مركز المقرر فيها شبيها بمركز الشاهد أين تكون الأقوال محل ثقة حيث توجب عليه قول الصدق.[471]

أما الصورية التي تقع بتغيير الحقيقة في محرر يتعلق بمصلحة يتفق عليها أطرافه فالفقه في ذلك على خلاف، حيث رأى البعض جواز ذلك كون أن المتعاقدين قد يريا مصلحتهما تقضي إضفاء ما يتفقان عليه و الأصل عند هؤلاء أن لا تقوم جريمة التزوير إن كانت البيانات غير الصحيحة التي تتبعها المتعاقدان في الفقه الظاهر تتعلق بخالص حقهما و مركزهما الشخصي فلا يعد إثباتها من قبيل تغيير الحقيقة الذي تتطلبه الجريمة.[472]

بينما رأى البعض أن الصورية التي لا تعد تزويرا هي التي تقع في المحرر وقت إنشاءه، إما إن تم تغيير الحقيقة بعد تمام المحرر، و يتعلق التغيير بحق الغير فإنه يعد تزويرا معاقبا عليه و لو وقع باتفاق الطرفين[473] و هذا مسلك من التعقيد بمكان.

أما إذا مست الصورية مركز الغير محرمة حقا ثبت له من قبل تمام تحريره أو بعده فإنه تغيير الحقيقة تقوم به جريمة التزوير.

مثال ذلك: تغيير الثمن في عقد البيع – بتخفيضه بعد تحرير العقد و ثبوت تاريخه رسميا بقصد انقضاء رسوم التسجيل – يعد تزويرا.[474]

نشير إلى أن عنصر تغيير الحقيقة تقوم به جريمة التزوير في المحرر الالكتروني يقع بعد خروجه على دعامة مكتوبة أو مسجلة و لا يعد تزويرا إذا تم الاعتداء عليه قبل خروجه كذلك.[475]

02 عنصـــر الضـــرر:

يعتبر الضرر أساسيا لقيام جريمة التزوير و الضرر هو التهديد و الاعتداء لكل مصلحة يحميها القانون كما يعرفه الفقه بأنه فقه أو نقص أو مساس بحال أو مصلحة يحميها القانون، و لا يميز في الضرر الذي يمس بالحقوق أو مصالح محمية بين الضرر المادي أو الأدبية كما يستوي أن يكون مساسا بمصلحة عامة أو خاصة كما أنه لا يلزم أن يكون حالا أو محتملا وقت تغيير الحقيقة.[476]

---

[471] - السقا ، مرجع سابق ، ص 51.

[472] - السقا ، مرجع سابق ، ص 51.

[473] - حسام أحمد حسام طه تمام ، مرجع سابق ، ص 389- 390.

[474] - نظرا في ذلك لارتباط حق آخر بالعقد عدا أطرافه و هو حق الخزينة العمومية في تقدير نسبة الرسوم و ارتباط تلك النسبة بالثمن الذي حدد في العقد وقت تحريره، السقا ، مرجع سابق ، ص 51.

[475] - حسام أحمد حسام طه تمام ، مرجع سابق ، ص 390.

[476] - حسام أحمد حسام طه تمام ، مرجع سابق ، ص 396.

و أي قدر من الضرر الفعلي هو الضرر المحقق أي الواقع فعلا و يعني وقوعه استعمال المحرر و هذا الأخير جريمة قائمة بذاتها، أما الضرر المحتمل فهو منتظر الوقوع وفقا لمجرى الأمور العادي، مع اعتبار أن تقدير احتمال الضرر إنما يكون بالوقت الذي وقع فيه تغيير الحقيقة في المحرر.[477]

كما أن تقدير وجود الضرر مسألة موضوعية متروكة للقاضي و يقدر الأخير قوة إثبات المحرر و الضرر المترتب عليه.[478]

03- عنصـــر المحـــرر:

يعد المحرر شرطا أساسيا في جريمة أو فعل التزوير سواء وجد قبل واقعة التغيير أي سبق من الفعل الإجرامي في الظهور أي أنه كان موجودا من قبل و غير الجاني بياناتها أو بعضها التي يتضمنها على نحو يجعلها مغايرة للحقيقة أو أنه كان متلازما مع الفعل الإجرامي الذي هو التغيير أي أنه قد أنشئ بأكمله من أجل تغيير الحقيقة به.[479]

و يقصد بالمحرر في الفقه الجنائي التقليدي بأنه " كل مكتوب يفصح عن الشخص من صدر عنه، و يتضمن ذكرا أو تعبيرا عن إرادة، من شأنه إنشاء مركز قانوني معين أو تعديله أو إنهائه أو إثباته، سواء أعد المحرر لذلك أساسا أو ترتب على هذا الأثر بقوة القانون "

أ/ طبيـــعة المحـــرر:

بحث طبيعة المحرر تكون و مدى ملائمته لوقوع جريمة التزوير فدرسها من جانبان:

ب/ قـــوة المحـــرر في الإثبـــات:

و هذا موضوع مجال دراسته القانون المدني و قد تناولته العديد من الدراسات و جانب ارتباطه بموضوعين هو أن البعض ربط الحماية الجنائية المقررة له بمدى قوته في الإثبات و هو رأي محترم في الفقه و القضاء حيث رأى أن التزوير لا يقع إلا في محرر فصلح لإثبات الحق أو واقعة ذات أثر قانوني حيث حسب رأيهم أن القانون يحمي الثقة التي يمكن أن يضعها الناس في المحرر و ليس في الكتابة ذاتها، و إذ الكتابة تعتبر دليلا في الإثبات[480]، و إن عارض البعض ربط التزوير بقوة المحرر في الإثبات على اعتبار أنها تطبيق شرط بلا سند إلى عناصر الجريمة، حيث لم ينص

---

[477] - السقا ، مرجع سابق ، ص 57.
[478] - حسام أحمد حسام طه تمام ، مرجع سابق ، ص 396.
[479] - حسام أحمد حسام طه تمام ، مرجع سابق ، ص 390.
[480] - حسام أحمد حسام طه تمام ، مرجع سابق ، ص 392.

الركن الشرقي إلا على تغيير الحقيقة في المحرر بطرق منصوص عنها محدة من شأنها إحداث ضرر أو احتماله.[481]

ج/ مـــدى تعـــادل المحـــرر الالكترونـــي بالورقـــي:

و الملاحظ في هذه المسألة هي تصور القواعد التقليدية الجزائية عن استيعاب فكرة المحرر الالكتروني و ملائمة تطبيق العقوبات المقررة لتزوير المحررات التقليدية (الورقية).

و هذا ما دعى بعض المشرعين إما إلى توسيع نطاق النصوص العقابية التقليدية كفرنسا مثلا م441 ق ع أو أفراد نصوص تشريعية خاص كما قد فعل المشرع المصري حيث فرض حماية قانونية للمحرر الالكتروني باستقلالية وضح لها مفهومه..... الجزاءات المترتبة على الاعتماد أو المساس بصحبة و سلامة[482].

ففي القانون رقم 15 لسنة 2004 بقانون التوقيع الالكتروني عرف المحرر الالكتروني في المادة 01 فقرة "ب" بأنه " رسالة بيانات تتضمن معلومات تنشأ أو تدمج، أو تخزن أو ترسل أو تستقبل كليا أو جزئيا بوسيلة الكترونية أو رقمية أو ضوئية، أو بأي وسيلة أخرى متشابهة "[483]

كما أعطى للمحررات الالكترونية في نطاق المعاملات المدنية و التجارية و الإدارية ذات الحجية المقررة للكتابة و المحررات الرسمية العرفية في أحكام قانون الإثبات في المواد المدنية و التجارية متى استوفت الشروط المنصوص عنها وفقا للضوابط الفنية و التقنية.

أما المشرع الفرنسي كما أسلفنا فقد توسع في مفهوم المحرر التقليدي ليشمل المحرر الالكتروني مع اشتراط إمكانية استخدام المحرر الذي تم تزويره لممارس ة حق أو تصرف، أو أن يصلح لإثبات حق تصرف له آثار قانونية[484].

الركن المعنوي :

---

[481] - حسام أحمد حسام طه تمام ، مرجع سابق ، ص 393.

[482] **Agathe LEPAGE, Réflexions de droit pénal sur la loi du 6 août 2004 relative à la protection des personnes à l'égard des traitements de données à caractère personnel, Revue Droit pénal n° 3, Mars 2005, Etude 5**

[483] - السقا ، مرجع سابق ، ص 55.

[484]- **Christophe CARON, Vers un droit pénal communautaire de la contrefaçon,** Revue **Communication Commerce électronique n° 6, Juin 2007, Repère 6**

المطلب الرابع : طــرق تزويــر المحــررات الالكترونيــة (تابع للتغيير):

و يقع التزوير المادي في المحررات الالكترونية بتغيير بيانات المحرر حذفا أو إضافة تطبيقا لما قضت به محكمة استئناف باريس بوقوع جريمة التزوير في المحررات من المتهم الذي غير تاريخ البرامج و المخزن على دعامة ليثبت نسبة البرنامج لنفسه لا لشركته التي كان يشتغل بها و عدل التاريخ بصورة التأخير كي يوهم أن البرنامج أعد بعد تركه العمل بالشركة لينفي أي سلطة لصاحب الشركة عليه.[485]

لكن قد يلجأ المشرع إلى إخراج بعض المحررات من قاعدة العامة على سبيل الاستثناء كما فعل المشرع الفرنسي باستثناء بطاقات الائتمان الممغنطة من القواعد العامة ليضبطها بنصوص خاصة ففي قانون 30 ديسمبر 1991 تضمن نصا يعاقب من قام باصطناع أو تزوير بطاقات الدفع أو السحب الخاصة.[486]

الفرع الأول : قصــور تشريعات طــرق التزويــر التقليديــة:

قد لا تتناسب تشريعات طرق التزوير التقليدية التي نصت عليها القواعد العامة لاحتواء الأساليب التقنية الحديثة المستخدمة و ذلك بسبب طبيعة المحرر الالكترونية فقد يعمد الجاني إلى محو البيانات عن طريق زرع فيروس أو برنامج دون إضافة بيانات أو قد يلجأ إلى تغيير كلمة المرور و استبدالها بأخرى و هذا من الصعب اعتبار كلمة المرور جزءا من المحرر الالكتروني و لعل هذا الأمر يحتاج إلى تخصيص مثل هذه الطرق بالنص[487].

01- خيــارات المشــرع:

من يرى المشرع خيارات تجاه التصدي لهذا النوع من الجرائم:[488]

أ/ الخيــار الأول: أن يعدل القواعد العامة في التزوير كي تنسحب على التزوير المحررات الالكترونية كالنهج الذي خطه المشرع الفرنسي في تعديل 1994 حينما استبدل المواد 145 إلى 152 في تزوير المحررات العرفية و أضاف إليها المواد

---

[485] - C. A Paris, 24 Mai 1996- Juris- Data. N° 021988، شيماء عبد الغني ، مرجع سابق ، ص عبد الغني 90.

[486] - رأى البعض أن هذا النص خاص يقيد العام، شيماء عبد الغني ، مرجع سابق ، ص عبد الغني 90.

[487] - شيماء عبد الغني ، مرجع سابق ، ص عبد الغني 91. **Christophe CARON, Vers un droit pénal communautaire de la contrefaçon, Revue Communication Commerce électronique n° 6, Juin 2007, Repère 6**

[488] - شيماء عبد الغني ، مرجع سابق ، ص عبد الغني 90.

625/462 المتعلقة بالغش المعلوماتي [489] التي جرمت تزوير الوثيقة المعلوماتية و استخدامها، و استبدل هذه المواد بنص المادة 441 التي أصبح حسب التعديل الجديد يستوعب التزوير العادي في المحررات بجانب تزوير الوثيقة المعلوماتية عندما أورد لفظ "بأي وسيلة كانت" و لفظ "أي سند أو دعامة (autre support)" و لم يحصر طرق التزوير تفاديا للإفلات من الوصف الإجرامي [490] مما لا يدع مجالا لشك في أن التعديلات المضافة في قانون العقوبات الفرنسي الجديد فعلت و أكدت حماية جنائية لأموال و نظام التجارة الالكترونية.[491]

ب/ الخيـــار الثانـــي: أن يورد نصا خاصا يعاقب فيه على تعديل أو تغير المحرر الالكتروني لجريمة مستقلة.[492]

الفرع الثاني : الطـــرق المعتمـــدة فـــي تزويـــر المحـــررات الالكترونيـــة:

حدد المشرع الجزائري الطرق المادية للتزوير على سبيل الحصر حيث لا تقوم جريمة التزوير إلا إذا كان مسلك الجاني بأحد هذه الطرق و قد بينت المادة 216 من القانون 06-23 المؤرخ في 20 ديسمبر 2006 بنصها:

"يعاقب بالسجن المؤقت من عشرة سنوات إلى ... ارتكب تزويرا في محررات رسمية عمومية":

إما بتقليد أو تزييف الكتابة أو التوقيع؛

و إما باصطناع اتفاقات أو نصوص أو التزامات أو مخالصات أو بإدراجها في هذه المحررات فيما بعد؛

و إما بإضافة أو بإسقاط أو بتزييف الشروط أو الإقرارات أو الوقائع التي أعدت هذه المحررات لتلقيها أو لإثباتها؛

و إما بانتحال شخصية الغير أو الحلول محلها.

كما يتعين على المحكمة ذات الموضوع عند الحكم بالإدانة، أن تبين الطريقة التي لجأ إليها الجاني في تغيير الحقيقة، و إلا كان حكمها قاصر التسبب متعين النقض.[493]

---

[489] - حجازي 356.

[490] - نص المادة حسام أحمد حسام طه تمام ، مرجع سابق ، ص 403.

[491] - حجازي 357.

[492] - شيماء عبد الغني ، مرجع سابق ، ص 90.

أنظر حجازي 18- 21

أنظر عبد القادر علي عبد القادر القهوجي ، مرجع سابق ، ص 38- 39- 40.

[493] - السقا ، مرجع سابق ، ص 60.

لكن ما نسجله هو عدم الإشارة الصريحة لإمكانية شمول هذه الجريمة للمحررات الالكترونية على غرار ما سطره بعض المشرعين فمثلا بعد أن أعطى المشرع المصري للمحررات الالكترونية في نطاق المعاملات التجارية ذات الحجية المقررة للكتابة و المحررات الرسمية و العرفية في القانون 15 لسنة 2004 الخاص بالتوقيع الالكترونية، أضاف القانون في المادة 23 منه فرض حماية قانونية على صحة المحررات الالكترونية، و أصبح عليها حماية معاقبة كل من "أتلف أو عيب توقيعا أو وسيطا أو محررا الكترونيا، أو زور شيئا من ذلك بطريق الاصطناع أو التعديل أو التحويل أو بأي طريق آخر"[494]

و تنقسم طرق التزوير إلى نوعان مادي و معنوي:

01- طــرق التزويــر المــادي: (يمكن الاستغناء عنه)

و يقصد بالتزوير المادي الفعل الذي يترك أثرا ماديا على العبث بالمحرر و يمكن أن يتبين هذا الأثر بالحواس المجردة و قد لا يتبين إلا بإعمال الخبرة و حصرت المادتان 214 من قانون 82-04 المؤرخ في 13 فبراير 1982 و المادة 216 من قانون 06-23 المؤرخ في 20 ديسمبر 2006 من قانون العقوبات الجزائري و تقابلها المادة 211 عقوبات مصري[495] و هي:

أ/ تقليــد أو تزيــف إمضــاء أو كتابــة:

و قد تطرقنا له سلفا يراجع.

ظهرت وسيلة مستحدثة في مجال التعاملات التجارية الالكترونية و هي متعلقة بوسائل الدفع عبر شبكة الإنترنيت أن يشترك في خدمات موقع الكتروني أو الحصول على سلعة فيه مقابل مبلغ متفق عليه من المال و تتم طريقة السداد بمثل طريقة الاستلام أي الكترونيا عن طريق الخصم من البطاقة الائتمانية بعد أن يسلم الموقع حافظة نقود الكترونية Cybex Cash Wallet في شكل برنامج Soft Ware و تخزن في ذاكرة جهاز العميل دون الحاجة إلى استخدام البطاقة الائتمانية.

فإذا ما تمكن أحد القراصنة من الوصول إلى هذا البرنامج و تغيير قيمته إلى الأعلى برفع سقفه، ثم استخدامه في الاستيلاء على الأموال بطريقة غير مشروعة، وقع التزوير في هذا المحرر الالكتروني.[496]

---

[494] - السقا ، مرجع سابق ، ص 61.

[495] - أنظر حسام أحمد حسام طه تمام ، مرجع سابق ، ص 393- 394.

[496] - السقا ، مرجع سابق ، ص 67.

02- الركـــن المعنـــوي:

يتطلب لقيام الركن المعنوي لجريمة التزوير توفر القصد الجنائي لدى الجاني بعنصرين القصد العام و الخاص و هي جريمة عمدية لا يعاقب عليها إلا إذا ارتكبت بقصد جنائي.

أ/ القصـــد العـــام (إرادة الفعل):

و فيه يكون الفاعل عالما بأنه يغير الحقيقة في محرر بإحدى الطرق التي بينها القانون مع توقع احتمال حدوث ضرر مادي أو أدى نتيجة الفعل.[497]

حيث يجب أن يعلم الجاني أنه يغير الحقيقة في المحرر و تنصرف إرادته إلى هذا التغيير و هذا القصد يتخلف و ينفى إذا ثبت أنه يجهل هذه الوقائع و لم تتجه نيته و لم يعلم بها، فلا بد لكي يقوم أن يتوقع الجاني كذلك احتمال وقوع الضرر نتيجة هذا التغيير و يعني أن يعلم الجاني أن فعله يسبب ضررا .... للمألوف و هذا لا يعني أن تكون إرادته قد انصرفت إلى إحداث الضرر[498].

القصد العام متمثل في "إدراك الفاعل أنه بفعله يخالف الموانع الشرعية بمعنى أنه يعلم أن ما يقوم به يعد تشويها للحقيقة"[499].

ب/ القصـــد الخـــاص (نية استعمال المزور):

يلزم بالإضافة إلى انصراف إرادة الجاني إلى ارتكاب الفعل المادي أن تتجه نيته وقت ارتكاب الفعل الجرمي إلى استعمال المحرر المزور فيما زور من أجله و هذه النية لازمة و تتجسد في الاحتجاج به على اعتبار أنه صحيح، و القصد الخاص يجب توفره في التزوير المادي و المعنوي.[500]

القصد الخاص متمثل في كون "الفاعل على وعي بأن ما يقوم به من شأنه أن يكون مصدرا للضرر"[501].

و قد استوعب نص المادة 441 عقوبات فرنسي كل طرق التزوير التقليدي أو الالكتروني.

المطلب الخامس : جريمـــة استعمـــال المحـــررات المـــزورة الكترونيـــا:

---

[497] - حسام أحمد حسام طه تمام ، مرجع سابق ، ص 397.
[498] - السقا ، مرجع سابق ، ص 59.
[499] - حسام أحمد حسام طه تمام ، مرجع سابق ، ص 441.
[500] - السقا ، مرجع سابق ، ص 59، حسام أحمد حسام طه تمام ، مرجع سابق ، ص 397.
[501] - حسام أحمد حسام طه تمام ، مرجع سابق ، ص 441.

نصت المادة 1/441-2 على العقاب على فعل استخدام المحررات المزورة و اعتبر المشرع استعمال المحرر المزور جريمة مستقلة عن جريمة تزوير المحررات حيث كل جريمة قائمة بذاتها، أي اعتبر من يستخدم محررا مزورا أيا كان و بأي وسيلة تم تزويره بعد جريمة استخدام باستعمال المزور فيما أعد له و يقصد تحقيق غرض ما و هو عالم بتغييره للحقيقة تلك يعاقب بالعقوبة المقررة في المادة في حالة استخدام محرر عرفي مزور، و تغلظ العقوبة حتى تصل إلى 07 سنوات سجن و 700.000 فرنك غرامة في حالة استخدام محرر رسمي مزور و المنصوص عليه في نفس المادة في الفقرة الثانية. و تكون المحررات الالكترونية عبارة عن دعامات.

الفرع الأول : الركـــن المـــادي:

نصت مختلف التشريعات على هذه الجريمة بتعبيرات متقاربة و على سبيل المثال أورد المشرع المصري في مادته 23 من القانون 15 لسنة 2004 الخاص بالتوقيع الالكتروني على معاقبة "كل من استعمل توقيعا أو وسيطا أو محررا الكترونيا معيبا أو مضر مع علم بذلك"[502].

و يلاحظ أن أركان هذه الجريمة هي فعل الاستعمال و محل الجريمة أي المحرر و لوجود العلم بذلك و هذا ما أحصاه الفقه أيضا و نستعرضها تبعا:[503]

01- الاستعمـــال:

الواضح من النصوص التشريعية سواء 441 ع فرنسي أو 211 ع مصري عدم حصر المشرع لطريق استعمال المزور مما جعل الفقه يتعرض لبيان أحكامه فعرفه بأنه التمسك بالمحرر المزور و الاحتجاج به بعد تقديمه إلى فرد معين أو إلى جهة معينة و بذلك يفترض في محل الاستعمال أمران: **الأول:** تقديم المحرر المزور، **الثاني:** الاحتجاج به.

أ/ تقديـــم المحـــرر المـــزور:

و يعني بتقديم المحرر المزور ذلك الفعل الإيجابي الذي يستخدم به المحرر المزور و الاستناد إلى دون فيه سواء أكان هذا الاستعمال قد تم أمام جهة رسمية أو مع موظف عام، أو أنه تم في إطار معاملات مع الأفراد.

ب/ الاحتجـــاج بالمحـــرر المـــزور:

---

[502] - السقا ، مرجع سابق ، ص 78.

[503] - السقا ، مرجع سابق ، ص 78.

لا يقوم الاحتجاج بمجرد استظهاره بل بما يستفاد منه انصراف نية الجاني إلى الاستفادة منه، فلو تخلفت إرادة الاستفادة من المحرر المزور لم تقم جريمة الاستعمال و لا يعد وجوده في ذاكرة حاسبة الآلي و لو أقر الشخص بذلك إذا ضبط عنده مشكلا لجريمة ما لم يقم دليل على أنه هو زوره.

و للقد أكد المشرع الجزائري أن في جريمة التزوير التقليدية أنه لا عقوبة على من تسلم المادة المزورة و هو يعتقد أنها صحيحة و استعمالها و الراجع في الفقه [504] أن الجاني يسأل إذا كان يعلم أن المحرر مزور حيث يتمثل فعل الاستعمال في إخراج الجاني المحرر المزور من حالة السكون السلبية إلى مجال التعامل مع علم بأنه بفعله يخالف الموانع الشرعية تتجه إرادته إلى دفعه للتعامل لتحقيق غرض ما زور لأجله.

02- المحـــرر:

بالنسبة للمحرر التقليدي الإشكال غير مطروح بالمقارنة إلى المحرر الالكتروني بالتساؤل مطروح ..... ما إذا كانت البيانات الموجودة في النظام أو على الدعامة من قبيل المحررات ثم إن المحرر الالكتروني يأخذ طابعا خاصا و قد سبق شرح ذلك لكن..... نقف عبر مميزات الكتابة الالكترونية.[505]

<u>الحمـــاية الجنائيـــة لأنظمـــة المعالجـــة الالكترونيـــة:</u>

ا/ خصائـــص الكتابـــة الالكترونيـــة:

أثبت الإشكالات المتعلقة بالمحرر الالكتروني فيما تعلق بالكتابة الالكترونية و ما يميزها عن الكتابة التقليدية ما يلي:[506]

تعكس الكتابة العادية شخصية محررها و ترتبط به ارتباط ينسبها إليه حين ندب الخبرة إلا أن الكتابة الالكترونية لا تفرق تبعا لكتابتها.

تتكون الكتابة العادية من حروف مكتوبة بأحبار سائلة و جافة بينما الكتابة الالكترونية و يترتب على ذلك إمكانية سهولة تعديلها.

تتطلب الكتابة الالكترونية وجوبا وسيطا للإطلاع عليها.[507]

---

[504] - السقا ، مرجع سابق ، ص

[505] - شيماء عبد الغني ، مرجع سابق ، ص عبد الغني 80.

[506] - شيماء عبد الغني ، مرجع سابق ، ص عبد الغني 81- 82.

[507] - فوزي السقا ، مرجع سابق ، ص 20.

هذه المميزات و غيرها جعل من القضاء و التشريع كلاهما يتوقف عن الإغراق للبيانات المبرمجة في الكمبيوتر أنها من قبيل المحررات في مفهوم التزوير (عدم الثبات، وجود واسطة القراءة)[508].

المحرر الورقي شيء مادي يمكن حسها ماديا بينما المحرر الالكتروني هو من قبيل الشيء الذي يحمل الطابع المعنوي و لا يمكن اعتباره ماديا مادام لم يستخرج.[509]

يختلف المحرران في العمر الافتراضي لكل منهما حيث الالكتروني هو الأطول عمرا و الأقوى سلامة.[510]

و توافر الركن المادي في جريمة التزوير يكفي لاعتبار المحرر المزور محلا لجريمة الاستعمال، لكن الركن المعنوي غير مشترط، لأنه انتفاء القصد لدى المزور لا يحول دون وقوع الاستعمال، حيث يعاقب المستعمل دون المحرر.[511]

الفرع الثاني : الركن المعنوي القصـــد الجنائـــي:

هذه الجريمة جريمة عمدية يأخذ ركنها المعنوي صورة القصد الجنائي العام و هو ان يعلم المتهم أن هذا (الوثيقة المعلوماتية) المحرر الالكتروني مزور الذي يتمسك به أي أنه يثبت علم الجاني اليقيني بتزوير المحرر و يستخدمها كدليل و يتمسك بها للحصول على حقوق قانونية بعد مرتكب الجريمة استعمال محرر مزور.[512]

و جريمة الاستعمال لمحرر يزور تنتفي بصفة عامة إذا ثبت جهل المتهم بتزوير المحرر كما أنه إذا لم تتجه إرادة الأخير إلى استعمال المحرر انتفى القصد الجنائي[513]

المبحث الرابع : حماية المستهلك في عقود التجارة الإلكترونية

أثار التعاقد عبر شبكة الإنترنيت العديد من الإشكالات القانونية وبخاصة ما تعلق منها بحماية المستهلك وهذا على إثر اختلالات تنظيمية في العلاقة التعاقدية من حيث اختلال التوازن بين المستهلك وبين الطرف المتعاقد الآخر باعتبار الأخير أقوى مركزا

---

[508] - شيماء عبد الغني ، مرجع سابق ، ص عبد الغني 82. **Thierry PIETTE-COUDOL, LCEN. L'écrit électronique et la signature électronique depuis la LCEN, Revue Communication Commerce électronique n° 9, Septembre 2004, Etude 29**

[509] - فوزي السقا ، مرجع سابق ، ص 20.
[510] - السقا ، مرجع سابق ، ص 21.
[511] - السقا ، مرجع سابق ، ص 81.
[512] - أحمد حسام طه تمام ، مرجع سابق ، ص حسام 445.
[513] - السقا ، مرجع سابق ، ص 82.

ثم من ناحية ثانية لكثرة استخدام وسائل الغش والخداع والتدليس في مثل هذه المعاملات.

وبقدر تطور هذه التجارة ينبغي أن يتلازم معه تطور النظام القانوني الضابط لهذه المعاملات، ولعل توفير الثقة للمتعاملين بهذه الوسيلة هو أحد سبل تطويرها ونمائها.

مما يستدعي توفير نظام قانوني حمائي للطرف الأضعف في هذه العلاقة ألا وهو المستهلك

توفر التجارة الإلكترونية فرصا فريدة للتبادلات التجارية العابرة للحدود، فهي تعد بمثابة أداة جديدة أحدثت تغييرا نوعيا على المنظومة الاقتصادية التقليدية على مستوى عالمي وإقليمي ومحلي، فهي تسمح للسلع والخدمات بأن تتوزع على سوق يتجاهل الحدود السياسية والجغرافية، وبقدر ما هي توفر فرصا كبيرة للشركات والمؤسسات، فإنها كذلك قوّت عاملي الإغراء والجذب للمستهلك وخاصة مع نماء معرفته التقنية باستخدام شبكة الإنترنيت وفتح الطريق أمامه إلى عالم التجارة الإلكترونية.

غير أن التعاقد عبر الشبكات الإلكترونية يثير العديد من الموضوعات المتعلقة بحماية المستهلك، فالتعاقد الإلكتروني مجال تتعدد فيه وسائل الغش والخداع، وإذ كان أساس حماية المستهلك في العقود كافة والعقد الإلكتروني بصفة خاصة يكمن في صفة حالة الضعف المسيطرة عليه واختلال التوازن بينه وبين الطرف المحترف الذي يقدم له السلعة أو الخدمة وهو الطرف الأقوى اقتصاديا والذي يفرض على المستهلك شروطه، فإنه من المشكوك فيه أن تصمد النظريات التقليدية لحماية المستهلك.

مما أثار التساؤل عن كيفية حماية المستهلك وعن نطاق هذه الحماية وهل تتلاءم القواعد التقليدية مع التكون الإلكتروني للعقد؟

المطلب الأول: مفهوم المستهلك الإلكتروني:

ونتعرف أولا على:

الفرع الأول : تعريف المستهلك الإلكتروني:

نقصد بمصطلح المستهلك الإلكتروني في مجال التعاملات أو التجارة الإلكترونية هو نفسه المستهلك في مجال العلاقات التعاقدية التقليدية، غير أن الفارق هو آلية التعاقد والتواصل بين الطرفين، حيث يتعامل المستهلك الإلكتروني في إطار تعاملاته التجارية

بوسيلة إلكترونية عن طريقة شبكة الاتصال العالمية (الإنترنيت) [514]، وهذا يعني أن للمستهلك الإلكتروني كافة الحقوق المقررة للمستهلك التقليدي.

وقد اختلفت التعريفات بين موسع ومضيق لمصطلح المستهلك ونأخذ كمثال لهذا الإختلاف تعاريف المشرع والقضاء والفقه الفرنسي، فقد عرف توجيه المجلس الأوروبي رقم 93/13 بتاريخ 1993/04/05 في المادة الثانية بشأن الشروط التعسفية في العقود المبرمة مع المستهلك عرف الإستهلاك بانه تلك العقود التي تبرم بين التاجر والمستهلك والتي يبرمها هذا الأخير بصفة عامة لأغراضه الشخصية وليس لأغراضه التجارية أو المهنية[515]، أما التوجيه الأوروبي رقم 97/07 فقد عرف المستهلك بأنه كل شخص طبيعي يبرم عقدا من تلك العقود التي تخضع لهذا التوجيه لأغراض لا تدخل في مجال نشاطه المهني، أما الفقه فقد عرف جانب منه المستهلك بأنه: الشخص الذي يبرم العقود المختلفة والمتنوعة من شراء وإيجار وقرض وانتفاع وغيرها من أجل توفير كل ما يحتاجه من سلع وخدمات لإشباع حاجاته الشخصية أو العائلية دون أن يقصد من ذلك إعادة تسويقها ودون أن تتوفر له الخبرة الفنية لمعالجة هذه الأشياء وإصلاحها، ومن التعريف الأخير يمكن أن نحصر شروطا ثلاث لإكتساب صفة المستهلك[516]:

أ/ أن يكون من الأشخاص الذين يحصدون أو يستعملون السلع والخدمات.

ب/ أن يكون محل الإستهلاك هو السلع أو الخدمات.

جـــ/ أن يكون الغرض من الحصول على السلعة أو الخدمة غرض شخصي وليس تجاري، يعني ذلك أن مفهوم المستهلك هو ذلك الشخص الذي يستغل السلع أو الخدمة لأغراضه الشخصية دون توفير نية تحقيق ربح في إطار معاملات استهلاكية.

فالمستهلك الالكتروني هو نفسه المستهلك في عملية التعاقد التقليدي مع إضافة خصوصية الوسيلة المستخدمة في التعامل ألا وهي شبكة الاتصال أي التعاقد عن بعد. كما تتحدد ملامح مفهوم وتعريف المستهلك وفق ما يلي[517]:

---

[514] هدى حامد قشقوش ، مرجع سابق ، ص حامد قشقوش، الحماية الجنائية للتجارة الإلكترونية عبر الإنترنيت، دار النهضة العربية، القاهرة 2000،ص65.

[515] خالد ممدوح إبراهيم محمد، إبرام العقد الإلكتروني، أطروحة دكتوراه، كلية الحقوق، جامعة الإسكندرية، 2005، ص334.

[516] المرجع نفسه، ص335.

[517] **عبد الفتاح بيومي حجازي ،التجارة الالكترونية وحمايتها الجنائية، الطبعة الاولى،الجزء الثاني،دار الفكر الجامعي،الاسكندرية ،ص ص 138-139**

1- الإستخدام الشخصي للسلع والخدمات : لما يحصل عليه المتعاقد من السلع و الخدمات بغرض الاستخدام الشخصي أي ما يمكن ان يعتمد عليه في حاجته الذاتية هو أو ذويه، وبذلك يخرج من هذا التعريف من يحصل على هذه السلع والخدمات بغرض إعادة تسويقها أو إستهداف الربح من إعادة البيع أو دمجها مع غيرها أي إمتداد الحلقة التعاقدية، فالمستهلك إذا هو من تنتهي عنده مسار السلعة او الخدمة الربحية.

2- عدم قصر المصطلح على الشخص الطبيعي بل يمتد ليشمل الأشخاص المعنوية كالشركات والمؤسسات عند لزوم هذه السلعة أو الخدمة المطلوبة للعاملين لديها أو منتجاتها او أداء مهامها.

3- تنوّع السلعة أو الخدمة : احتياجات المستهلك غير مقصورة على مجال دون غيره أو سلعة دون أخرى فقد تتوزع بين سلعة أو اخرى وقد تتنوع بين مأكل، مشرب، ملبس، نقل، صيانة، تامين، علاج، استشارت [518].

4- متى يكون المهني أو المحترف مستهلك : الأصل أن الشخص الذي يحصل على سلعة اوخدمة متعلقة بمهنته بمقابل لا يعتبر مستهلكا والعبرة في عدم استفادته من الحماية المقررة للمستهلك هي توفر الخبرة الكافية لحماية نفسه من أي غش أو خداع إلا ان هذا الحكم وإن كان قاعدة فإن لها استثناءت فعندما يتعاقد هذا المهني او المحترف للحصول على سلعة لا تدخل في نطاق مهنته التي يحترفها يعد في هذه الحالة مستهلكا.

الفرع الثاني : دواعي توفير الحماية للمستهلك الإلكتروني:

أصبح المستهلك في ظل الإقتصاد الرقمي عرضة للتلاعب بمصالحه وعرضة للغش والخداع بواسطة التضليل والايهام بمزايا غير مطابقة للحقيقة وبرغم المخاطر التي تتهدد مركزه الضعيف في العلاقات التعاقدية الالكترونية إلا ان المشرع العربي لم يهتم بدرجة كافية بتأمين حماية له مقارنة بالمشرع الأجنبي [519]، مع النظر لطبيعة المعاملة الالكترونية التي توسع من إمكانية التعسف من قبل المهني أو المحترف لعدم التوازن العقدي بين الطرفين.

---

[518] اي تنوعها بين الحاجات الذاتية، المادية، المالية، الفكرية.

[519] - **Nicolas MATHEY ,Le commerce électronique dans la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, Contrats Concurrence Consommation n° 10, paris,Octobre 2004, Etude 13**

عبد الفتاح بيومي حجازي ،التجارة الالكترونية وحمايتها الجنائية، مرجع سابق، ص **137** .

وبفعل التطور الحاصل في وسائل الإتصال وانتشار المعاملات الإلكترونية أصبح المستهلكون غير مقيّدين بحواجز مكانية أو زمانية وبحكم أن طرفي العلاقة التعاقدية التجارية أحدهما في مركز قوة ألا وهو المهني أو المحترف الذي يقدم السلعة أو الخدمة كما أنه يفرض شروطه على المستهلك الذي لا تتواجد السلعة بين يديه إنما يشاهدها عن طريق وسائل دعاية (شبكة الإنترنيت)، وبالضرورة أحيانا قد يكون المهني أو المحترف أجنبيا أو يقيم أو يتعامل مع المستهلك من بلد أجنبي، فإننا نجد أن المستهلك هو الطرف الضعيف في التعاقد الذي يسيطر عليه حالة من الضعف مما تضفي حالة اختلال في التوازن بين طرفي العلاقات التعاقدية ومن المفارقات أنه لا تزال في بعض التشريعات تعتمد القواعد القانونية التي تحكم النشاط الإستهلاكي هي النظريات التنقليدية للإلتزامات، ولن تتصدى هذه النظريات لحماية المستهلك الإلكتروني[520]، بينما استهدفت بعض التشريعات الوطنية بيان النظام القانوني لحماية المستهلك بما يمكن أن يخفف من ذلك الإختلال بين مصلحة المنتج أو المهني وبين مصلحة المستهلك[521].

الفرع الثالث : نـــطاق الحماية :

تشمل حماية المستهلك الإلكتروني في الفقه عدة مراحل فتبدأ بمرحلة التفاوض، مرحلة إبرام العقد، مرحلة تنفيذ العقد، مرحلة خدمة ما بعد البيع، وتتضافر جهود المشرع لحماية المستهلك الإلكتروني بتوزع قواعد هذه الحماية على اكثر من قانون(القانون الجنائي، التجاري، المدني،قانون الاستهلاك...).

فالقانون الجنائي:

يسعى إلى حماية المستهلك عن طريق قمع الغش، قمع الاحتكار، محاربة التهريب، كف الإعتداء على البيانات الشخصية، التنصت، المعاملات المالية، حماية التوقيع الالكتروني: وسائل الدفع الالكترونية وغير ذلك.

أما القانون المدني:

فيسعى الى حمايته عن طريق توفير كافة الضمانات القانونية لحمايته من السلع غير المطابقة للمواصفات وتبصير المستهلك بكافة جزئيات التعاقد لمنعه دون الوقوع في

---

520 أسامة أحمد بدر، حماية المستهلك في التعاقد الإلكتروني، دارسة مقارنة، دار الجامعة الجديدة للنشر،الاسكندرية،**2005**،ص**31**

521 خالد ممدوح إبراهيم محمد، مرجع سابق، ص**329**

الخطأ، كتبصيره بسعر السلعة، طريقة الوفاء، طريقة التسليم الصيانة وخدمات مابعد البيع، الجهة المحكّمة [522].

وعموما فإن مختلف التشريعات الوطنية وبحكم حداثة التعامل بهذه الآلية لم تفرد قواعد حمائية مستقلة خاصة بمركز المستهلك الالكتروني نجد أننا نستطيع أن نستطلع قواعد قانونية في التشريعات المقارنة واجتهادات المشرعين بخصوص هذا الوافد.

المطلب الثاني : قواعد حماية المستهلك في التشريعات المقارنة [523]:

ما تجدر الإشارة إليه أن العديد من التشريعات الوطنية اهتمت بحماية مركز المستهلك وللأسف ليس الحال كذلك بالنسبة لأكثر الدول العربية، فربما كان ذلك بسبب عدم نماء أساليب التجارة الإلكترونية في الأوطان العربية، غير أن المستهلك في الدول العربية غير منعزل عن التعاملات الإلكترونية في إطار تعاملاته الإستهلاكية وهو ما يضطر المشرع العربي ويدعوه جديا إلى المبادرة إلى فرض حماية له وتقنينها على غرار المشرع الغربي، والمشرع التونسي وقانون إمارة دبي الذي يمكن أن نرى أو أن نتعرض له بشيء من الشرح حيث بادرت هذه الدول بتضمين تشريعاتها الخاصة بمعاملات التجارية الإلكترونية نصوص خاصة بحماية المستهلك.

الفرع الأول : قانون التجارة الإلكترونية لدوقية لوكسمبورغ وإيطاليا:

تضمن هذا القانون بعض الجوانب المتصلة بالحماية المسبقة منها إعلام المستهلك بالمعلومات الخاصة بالمورّد وبمواصفات السلع والمنتجات والخدمات والعملة التي يتم بها السداد ومدة العرض وحق المستهلك في العدول عن التعاقد أما قانون التجارة الإلكترونية بإيطاليا فألزم الموردين إعلام المستهلكين بالمواصفات التفصيلية للبضاعة أو الخدمة بما فيها الضرائب الإلكترونية قبل إبرام العقد.

الفرع الثاني : قانون الاستهلاك الفرنسي:

تضمن قانون الاستهلاك الفرنسي رقم 949 / 93 الصادر بتاريخ 26 يوليو 1993 نصوصا تتعلق بإعلام المستهلك وحمايته وتنظيم جمعيات المستهلكين التي تنشط في مجال حماية المستهلك بفاعلية تكاد تكون محققة لهدف وأغراض النصوص القانونية إلا أن المستهلك في مجال التجارة التقليدية يتمتع بحماية أكبر من المستهلك الإلكتروني من الناحية التشريعية.

---

[522] خالد ممدوح إبراهيم محمد، مرجع سابق،، ص**331**.

[523] يونس عرب، موسوعة القانون الالكتروني.الموقع = **arablaw.org**

الفرع الثالث : القانون التونسي للمعاملات الإلكترونية:

فصل المشرع التونسي في القانون الصادر سنة 2000 بشأن معاملات التجارة الإلكترونية الذي يعتبره البعض قانونا متميزا بما حواه مجموعة من القواعد الضابطة لهذه المعاملات ففيما يتعلق بحماية المستهلك فقد خصص المشرع التونسي الباب الخامس من ذات القانون لحماية المستهلك وتكفلت المادة 25 منه بإالزام البائع أن يبين بوضوح للمستهلك في العقد الإلكتروني البيانات التالية[524]:

- هوية وعنوان وهاتف مقدم الخدمة.
- وصفا كاملا لمختلف مراحل إنجاز المعاملة.
- طبيعة وخصائص وسعر المنتج أو الخدمة.
- كيفية تسليم السلعة ومبلغ التأمين المستحق منه في الحال
- الفترة التي تكون خلالها السلعة أو الخدمة معروض بالأسعار المحددة.
- شروط الضمانات المقدمة وعقد البيع الإلكتروني وخدمة ما بعد البيع.
- طرق وإجراءات الدفع، وعند الاقتضاء وشروط القروض المقترحة.
- طرق وآجال التسليم وتنفيذ ونتائج عدم إنجاز الإلتزامات.
- إمكانية العدول عن الشراء وأجله.
- كيفية إقرار الطلبية أي إرسال الموافقة على صيغة البيع.
- استعمال تقنيات الإتصال
- شروط فسخ العقد
- المدة الدنيا للعقد فيما يتعلق بالعقود الخاصة بتزويد المستهلك بسلعة أو خدمة خلال مدة طويلة أو بصفة دورية.

الفرع الرابع : حمايـــة المستهلك في قانون إمارة دبي

كافئ مشرع إمارة دبي حماية المستهلك في التجارة التقليدية والمستهلك الإلكترونية، كما انه ركز على الحد مما يلي:

محاولات الإحتيال والنصب على المستهلك كحالات تزوير المراسلات الإلكترونية

عاقب على جرائم تزوير شهادات التصديق الإلكترونية.

عاقب على نشر هذه الشهادات والبيانات الإلكترونية بقصد الإحتيال على الآخرين

---

[524] عبد الفتاح حجازي، مقدمة في التجارة الإلكترونية العربية، الجزء الثاني، دار الفكر الجامعي، الاسكندرية، **2004**، ص **118**.

عاقب كل من يقدم بيانات شخصية زائفة ويترتب عليها الإضرار بالغير في نطاق التجارة الإلكترونية.

نظم حقوق أطراف العقد من حيث تحديد مكان وزمان انعقاد العقد.

نظم وسيلة تحقق المستهلك من صحة توقيع المنتج أو البائع المحترف أو التاجر عن طريق التوقيع الإلكترونية المحمي قانونا ضمن المواد 20 و21 وما بعدهما.

التأكيد على وجود طرف ثالث (وسيط) بين المستهلك والطرف الآخر في العلاقة الإلكترونية ووظيفته التصديق على صحة بيانات المعاملة الإلكترونية [525].

ونضمت المادة 25 من القانون ذاته عمل مزود خدمات التصديق[526].

ويعدّ البعض[527]أن أهم الأحكام التي إحتواها هذا القانون ما تضمنته المادة 21 والتي نصت على عقاب كل من أفشى سرا اطلع عليه بحكم عمله بالحبس والغرامة أو أحدهم سواء كان ذلك عن قصد أو حتى إن حدث نتيجة إهمال أو عدم إحتياط وذلك تأكيدا لحماية الخصوصية والبيانات الشخصية والحيلولة دون كشف الأسرار، ومن باب الإحتياط عاقبت المادة 32 كل من كانت وسيلته (لإرتكاب الجريمة وسيلة إلكترونية) كل من تصنف جريمته أنها جريمة إلكترونية كحالة تقليد السلعة أو الغش أو التلاعب في خواصها بوسيلة إلكترونية وفي حال أن كانت هذه السلعة أو الخدمة قد تم التعاقد عليها بوسيلة إلكترونية فإن الحماية الجنائية مشمولة بالنص السابق ودائما لمصلحة المستهلك.

الفرع الخامس : حماية المستهلك في قانون التجارة الإلكترونية المصري :

خصص المشرع المصري الفصل السابع من قانون التجارة الإلكترونية لقواعد حماية المستهلك وتمثلت هذه الحماية في ضمانات حقيقة من شأنها أن تقي المستهلك من مخاطر العملية التعاقدية الإلكترونية وأهم هذه النقاط تمثلت في[528]:

---

[525] عبد الفتاح حجازي، مقدمة في التجارة الإلكترونية العربية، مرجع سابق ،ص225..

[526] **الوسيط هو ذلك الطرف الذي يبصدق على صحة بيانات المعاملة الإلكترونية حتى تكتسب هذه المعاملة ثقفة أطرافها وتحوز يقينهم من فهم المستهلك وقد حددت المادة 24 من نفس القانون على واجبات مزود خدمات التصديق،عبد الفتاح بيومي حجازي، حماية المستهلك عبر شبكة الإنترنيت، الطبعة الأولى ، دار الفكر الجامعي، الإسكندرية، 2006 مرجع سابق، ص-ص 36/35**

527 عبد الفتاح بيومي حجازي، حماية المستهلك عبر شبكة الإنترنيت، مرجع سابق ،، ص 36، حجازي، مقدمة، ص225.

[528] هدى حامد قشقوش ، مرجع سابق ، ص حامد قشقوش، مرجع سابق.، ص67.

ذكر البيانات الهامة عند الإعلان عن السلعة أو الخدمة عبر الوسائطة الإلكترونية حماية للمستهلك من الجهل والغرر والتضليل عند إبرام العقد الإلكتروني.

حضر نشر أو التعامل بالبيانات الشخصية أو المصرفية للمستهلك من أي جهة كانت إلا بموافقة صاحبها موافقة كتابية.

أقوى عنصر في هذه الحماية التي قررها المشرع المصري هي تلك التي صنف فيها العقود النمطية إلكترونيا من عقود الإذعان وهو ما يعني تفسيرها لصالح الطرف المذعن (أي المستهلك) وجواز إبطال ما يرد فيها من شروط تعسفية وإعتبار أي شرط يخل بالتوازن المالي للعقد من قبيل الشروط التعسفية التي يجوز بموجب هذا القانون المطالبة بإبطالها.

أعطى الحق للمستهلك في فسخ العقد بإرادته المنفرد خلال 15 يوم من تسلمه المنتج أو الخدمة دون التسبيب للفسخ.

المطلب الثالث : بعض صور الحماية الجنائية للمستهلك:

نتكلم عن بعض تلك الأوجه التي تدخلت البعض من التشريعات لضبطها وتقرير صور حمائية لها و بالأخص الحماية الجنائية على سبيل المثال:

الفرع الأول : الحماية الجنائية لبيانات المستهلك الشخصية :

أثار تعاقد المستهلك الإلكتروني العديد من المشاكل بشأن حمايته القانونية وأهم هذه المشاكل التي أثارها مشكل الإطلاع على بياناته الاسمية والشخصية المقدمة أثناء أو قبل إبرام العقد أو التي يتوصل إليها عن طريق الإنترنيت أثناء الكشف عن رغباته وقد أثار تحديد مفهوم البيانات الشخصية خلافا في الفقه القانوني حيث يرى البعض أن هذه البيانات هي تلك المتعلقة بحياة الفرد الخاصة (حالته الصحية، المالية، المهنية، الوظيفية، العائلية) بينما رأى البعض أنها متفرعة إلى صور منها بيانات متعلقة بحرمة الحياة الخاصة للفرد، ومنها بيانات عند استخدامها يمكن أن ترسم صورة لاتجاهات وميولات الإنسان، وصورة متعلقة باتجاهاته السياسية ومعتقداته الدينية وتعاملاته المالية والبنكية وجنسيته وهواياته، وقد اتجه المشرع الأوروبي إلى تأكيد حماية أكبر في هذا النطاق فقد أكد التوجيه الأوروبي رقم 46/95 الصادر في 1995/10/24 بشأن حماية الأشخاص الطبيعيين عند معالجته البيانات الشخصية وحرية تداول هذه البيانات على ضرورة حماية الحقوق الأساسية وبخاصة الحق في حرمة الحياة الخاصة (المادة 01/ الفقرة 01) وأكد على حق المواطن في الإطلاع على البيانات المتعلقة به (المادة 12)،

وحقه في الإعتراض (المادة 14) وحقه في سريتها وتأمينها (المادة 16، المادة 17)[529].

الفرع الثاني : الحماية الجنائية ضد الغش التجاري والصناعي :

يعرف الغش التجاري والصناعي بأنه" كل فعل من شأنه أن يغير من طبيعة أو خواص المواد أو فائدتها التي دخل عليها عمل الفاعل، ولا تهم الوسيلة التي لجأ إليها الفاعل في سبيل تحقيق غايته، فقد يتم الغش بإحلال مواد أقل قيمة مكان أخرى أعلى منها في ما يراد، وإدخال الغش عليه، أو بإنقاص بعض المواد أو إضافة مواد أخرى عليه تزيد من كميته وتقلل من مفعوله، وغير ذلك للحصول على أرباح طائلة وغير مشروعة "[530].

وقد يقع الغش بفعل الإنسان أو قد يكون لأسباب لا دخل لإرادة الإنسان فيها كفساد سلعة أو فوات آجال استهلاك ومنه نقول أن للغش ركنان مادي ومعنوي [531] أما المادي فيتحقق بأحد الأفعال الآتية :

- الغش أو الشروع فيه أو فساد المادة.
- بيع أو عرض المواد المغشوشة أو الفاسدة.
- التحريض على استخدام هذه المواد في الغش.

أما الركن المعنوي فيتحقق في هذه الجريمة بانصراف إرادة الفاعل إلى تحقيق الواقعة الجنائية مع العلم بتوافر أركانها في الواقع، أي توفر نية الغش ويتعين توفرها وقت وقوع الفعل بأن جريمة الغش من الجرائم العمدية الوقتية ويلحق بهذه الجريمة حالات الغش والتقليد في مراحل الإنتاج الصناعي وتقليد العلامات التجارية المضللة للمستهلك (القانون 1993/57. دولة الإمارات) حتى تصل إلى البيانات التجارية وكذا عند تعبئة وتجهيز المنتج الصناعي.

الفرع الثالث : جريمة الاحتيال في عقود التجارة الإلكترونية :

يكاد يكون الاحتيال السمة الغالبة على معاملات التجارة الإلكترونية ويقع في وسيلة الربط بين المستهلك وبين السلعة أو الخدمة وهذه الوسيلة هي الدعاية فالمنتج عادة ما

---

[529] أمين اعزان، الحماية القانونية للمستهلك في مجال التجارة الإلكترونية عبر شبكة الإنترنيت ــ رسالة ماجيستير في القانون التجاري، معهد البحوث والدراسات العربية بالقاهرة 2003، ص 112 –115، انظر ايضا:

-La protection juridique des bases des donnees electroniques, petites affiches LPA, france 28 avril 1995, n° 51 , , P. 14

[530] عبد الفتاح بيومي حجازي، حماية المستهلك عبر شبكة الإنترنيت، مرجع سابق، ص 58.

[531] المرجع نفسه، ص60.

يعتمد أساليب ترويج لتسويق منتجاته وتوزيعها بدعاية غير مطابقة لمواصفات السلعة أو الخدمة الحقيقية وعادة ما تحتوي على مغالطات تضلل المستهلك وتدعوه كمحفز للتعاقد بهدف تحقيق أقصى قدر من الربح.

فالمستهلك في ظل تطور وسائل الإتصال ونماء تعاملات التجارة الإلكترونية يبقى دائما عرضة للتلاعب بمصالحه وتزيد محاولة غشه وخداعه، فالمهني في سبيل تحصيله على الربح السريع ينزع إلى تسويق منتجاته بأساليب غير مشروعة ليضلل المستهلك بها ويخدعه بإيهامه بوجود مزايا لا تتوفر عليها السلعة أو عدم توفير متطلبات الأمن والسلامة في المنتج كما يستدعي توفير حماية للمستهلك في هذه البيئة الإلكترونية[532] وقد تضمن قانون الإستهلاك الفرنسي الصادر عام 1993 نصوصا تحارب الغش والخداع في طائفتين من الأفعال.

الطائفة الأولى: نضمتها المواد 4/121 وما بعدها وعاقبت كل من يقوم بالدعاية الكاذبة أو التي من شأنها الإيقاع في الغلط..

الطائفة الثانية: نضمتها المواد 1/213 وما بعدها وعاقبت على الغش والتدليس.

وفي كل النصوص والطائفتين تتبع النصوص التجريمية بالحبس والغرامة أو إحدى العقوبتين مع إمكانية إضافة عقوبات تكميلية [533]، ولتدعيم هذه الحماية اكدت مختلف التشريعات على تاكيد آخر للمستهلك من شانه ان يكفل حماية له.

الفرع الرابع : الحق في الإعلام:

يعني الحق في الإعلام ان يلتزم المتعاقد بأن يمد الطرف الاخر بكل معلومة أن تساعده في اتخاذ القرار بخصوص العقد وهذا الحق يدرج كشرط ضمن العقود التجارة الالكترونية ويعني إعلام المستهلك بالمنتاجات المعروضة وبقوانين المعلومات والحريات كما يمكن أن يشمل إعلام العميل بالاعباء الضريبية والجمارك وتحرص بعض التشريعات في إطار تقرير وتفعيل الجانب الوقائي لحماية المستهلك على إعلام المتعاقد بقانون حماية المستهلك على كافة القواعد القانونية المقررة لحمايته في حالة الإقتدام على التعاقد حتى يكون المستهلك على بصيرة من أمره قبل وأثناء تعاقده وهذا

---

[532] خالد ممدوح إبراهيم محمد، مرجع سابق،، ص**331**، انظر ايضا:

-Éric A. CAPRIOLI, Mesures techniques de protection et d'information des droits d'auteur, Communication Commerce électronique n° 11,paris,France, Novembre 2006, Etude 30

[533] عبد الفتاح بيومي حجازي، حماية المستهلك عبر شبكة الإنترنيت، مرجع سابق ،، ص **60–61**.

الحق لم تشمله قواعد القانون المدني فقط بل شملبته قواعد القانون الجنائي كالالتزام بعدم الغش وترتب المسؤولية الجنائية على عدم مراعاة هذا الالتزام [534].

فبالإضافة إلى حق المستهلبك في الإعلام الرئيسي المتعلق بالمنتجات المعروضة وثمنها نجد في عقود التجارة الالكترونية شروطا أخرى منها الإعلام بقوانين المعلوماتية والحريات وهو حق مكفول للمستهلك في فرنسا القانون 17 /78 الصادر في 06 يانير 1978 الخاص بالمعلوماتية والسجلات والحريات أن يكون المستهلك بموجبه الحق في الإطلاع على بياناته الخاصة كما حضر هذا القانون الاحتفاظ بالبيانات الخاصة ببطاقته المصرفية خارج مدة التعامل مع الطلب أن بيانات التعريف بالمستهلك لا يجوز نقلها من متجر إلى آخر غير الذي تعامل معها إلا بناءا على طلبه [535].

وقد تصدى لهذه المسؤولية التوجيه الأروبي 97/66 الصادر في 15 ديسمبر 1997 الخاص بمعاملة البيانات ذات الطابع الشخصي وحماية الحياة الخاصة في قطاع الاتصالات ويعد الإخلال بالالتزام بالاعلام إخلالا بالتزام تعاقدي في القانون الفرنسي قد يؤدي إلى فسخ العقد وتترتب عنه مسؤولية تعاقدية كما يمكن للمستهلك الذي أصابه الضرر حق المطالبة بتعويض متى كان لهذا التعويض مقتضى[536].

كما يمكن أن تقوم مسؤولية جنائية اتجاه المتعاقد عندما يثبت استخدامه وسائل الخدع والحيل تدفع المستهلك إلى التعاقد حسب قواعد قانون التجارة والمبادلات الالكترونية التونسي الصادر في عام 2000 [537].

الفرع الخامس : الصـــور الأخرى للحماية الجنائية للمستهلك الإلكتروني :

---

[534] عبد الفتاح بيومي حجازي ،التجارة الالكترونية وحمايتها الجنائية، مرجع سابق، ص**154**.

[535] أسامة أبو الحسن مجاهد، التعاقد عبر الانترنيت **2005** . دار الكتب القانونية، ص ص **108 –109**

[536] عاقب المشرع الفرنسي على الدعاية الكاذبة وجعل من صلاحيات وكلاء الضرائب ووكلاء الغش والضبطية القضائية تقديم محاضر تشمل دليل عن الدعاية الكاذبة إلى النيابة العامة وللمحكمة أن تأمر بتصحيح الإعلام حسب تكييف المحكمة للوقائع وإن كانت طبيعة الدعوة تحريض المستهلك على الغلط فإن عقوبتها فعل ممارسة السعر الغير المشروع، أنظر الفتاح بيومي حجازي ،التجارة الالكترونية وحمايتها الجنائية، مرجع سابق ،ص**154** .

[537] نصت المادة **50** من هذا القانون :يعاقب كل من يستغل ضعف أو جهل شخص في إطار عمليات البيع الالكتروني بدفعه الالتزام حاضرا او أجلا بأي شكل من الأشكال بخطية تتروح بين **1000** و **20** الف دينار وذلك إذا ثبت من ظروغ الواقعة أن هذا الشخص غير قادر على تميز أبعاد تعهداته أو كشف الحيل والخدع المتعمدة بالالتزام أو إذا ثبت أنه كان تحت الضغط مع مراعاة احكام المجلة الجنائية وائل بندق ، موسوعة القانون الالكتروني وتكنولوجيا الاتصالات، دار المطبوعات الجامعية ،الاسكندرية**2007**، ص **966** .

كما يمكن أن نخص أنواعا أخرى شملتها قواعد التشريعات المقارنة التي يمكنها أن توفر حماية فاهلة للمستهلك الإلكتروني ومنها [538]:

– تحريم الدخول غير المشروع للمواقع الإلكترونية (التجارب الخاصة) للحصول على بيانات المستهلك.

– خطر التعامل في البيانات الشخصية أو الإسمية للمستهلك دون إذن.

– حماية وسائل الدفع الإلكترونية من التعدي عليها.

– تجريم إنتهاك سرية وخصوصية بيانات المستهلك.

– تجريم التعدي على التوقيع الإلكتروني أو البيانات المشفرة للمستهلك.

– تجريم التعدي على بيانات بطاقات الإئتمان الخاصة بالمستهلك.

– تجريم تزوير المحررات الإلكترونية التي يكون المستهلك طرفا فيها.

الخاتـــمـــة

رأينا أن تحديد نطاق حماية المستهلك وتشريع قوانين ونصوص ضابطة لهذه الحماية يتوقف على تحديد مفهوم أو معنى الإستهلاك أولا، ذلك أن الإستهلاك هو ثقافة ونشاط اجتماعي [539]، كما أنه ممارسة غير مقتصرة على فئة دون أخرى أو طائفة دون غيرها إنما هو في عداد الثقافة العامة.

غير أنه على المشرع العربي أن يولي عناية كافية لحماية مراكز المستهلكين على الأقل في إطار انعكاس ثورة المعلومات على العديد من المراكز القانونية ووجوب تغيير أو تعديل قواعد الحماية التقليدية على غرار المشرع الأجنبي

يتضح جليا أن ثورة المعلومات تفوق جهود المشرع أينما كان فلم تفي كافة المحاولات التي بذلت من قبل رجال الفقه ولا إجتهادات القضاء والمشرعين للإحاطة بأحكام ضابطة للمعاملات الإلكترونية حيث لا تزال الكثير من المصطلحات تحتاج إلى ضبط

---

[538] عبد الفتاح حجازي، التجارة الإلكترونية وحمايتها القانونية ،مرجع سابق، ص13 ،انظر أيضا:

-Thierry PIETTE-COUDOL ,L'écrit électronique et la signature électronique depuis la LCEN, Communication Commerce électronique n° 9, paris,Septembre 2004, Etude 29 LCEN.

-Agathe LEPAGE, Libertés sur l'Internet et cybercriminalité : les apports au droit pénal de la loi pour la confiance dans l'économie numérique du 21 juin 2004, Droit pénal n° 12, Décembre 2004, Etude 18

[539] ولعله أول وأكبر نشاط تمارسه مجتمعاتنا الغير منتجة ويكاد يكون أو هو بالاحرى ثقافة عامة وميزة تنافسية .

أكبر، فالتجارة الإلكترونية بصفة عامة لا بد لها من بيئة قانونية مضبوطة كي تضمن حقوق ومصالح كل أطرافها المتعاملين فيها، وليس يجدي نفعا الإكتفاء بتضمين القوانين التقليدية مجموعة نصوص إضافية وإدخال تعديلات بقدر ما يكون الحل الأنفع هو الإجتهاد في وضع قانون مستقل للمعاملات الإلكترونية. اما بالنسبة للمشرع العربي على وجه الخصوص فعليه ان يولي عناية خاصة بمركز المستهلك.

الباب الثاني:

الحماية الجنائية الإجرائية

للتجارة الالكترونية

تمهيد:

إن تطور التقنيات الحديثة كانت دائما مصدر جذب لعناصر لم يتورعوا في تسخير نشاطهم الفكري و تصوراتهم العقلية لتحقيق أهدافهم اللامشروعة، فالمعلوماتية لم يفقد أصحابها السيطرة عليها و التحكم في مسارات أهدافها فحسب، بل إن آليات المعلوماتية استخدمت لأغراض إجرامية، وهذه الشبكات تنمو و تتضاعف و الظاهرة في تطور, مما جعل تعرض المعاملات الالكترونية لهذه الاعتداءات هو أكبر خطر يهدد مستقبل الفضاء الرقمي (الاقتصاد، الإدارة، المجتمع)، إذ هو في حاجة لإجراءات واسعة لحماية فعالة لهذه المعاملات[1].

ينبغي أن يستوفى موضوع الحماية الجنائية للتجارة الالكترونية بدراسة الجوانب الإجرائية لهذه الحماية، و هذه ما تضمّنه الباب الثاني من هذه الدراسة. حيث اجتهد في الإحاطة بالأحكام الإجرائية بتقسيم هذا الباب إلى ثلاثة فصول.

فخصّص الفصل الأول لدراسة بعض الجوانب الإجرائية لجرائم التجارة الالكترونية المتعلقة بطبيعة عمل السلطات القضائية من رجال ضبط و هيئات تحقيق, أما الفصل الثاني فأدرج لبحث إشكالات الجوانب الإجرائية أثناء مرحلة المحاكمة و بيان المشكلات التي يثيرها إجراء التفتيش و الضبط بصفة حصرية دون غيرهما و مدى حساسيتهما فيما يتعلق بهذه التقنية أو الآلية الرقمية.

و الفصل الثالث تركّز على التجارب الدولية في مجال مكافحة الجريمة من هذا النوع بالأخص فيما طرحته الجوانب الإجرائية من إشكالات و ذلك باستعراضها في ضوء الاتفاقيات الدولية، و بعدها تطرقنا لدور التعاون الدولي في الحدّ من هذه الظاهرة كون الجرائم الواقعة على التجارة الالكترونية من الجرائم العابرة للحدود.

[1] - André prum,op.cit, p327.

الفصل الاول

الطبيعة الخاصة

للجريمة في بيئة التجارة

الالكترونية

فقد أمست الجرائم المعلوماتية من أخطر الجرائم التي ترتكب عبر العالم ، ذلك أن هذه الجرائم حاليا تنوعت أساليب ارتكابها و تزايدت مخاطرها وحجم الخسائر الناجمة عنها. ولهذا فمع إدراك خطورة و سهولة ارتكاب هذه الجرائم الجديدة التي أفرزتها بيئة المعالجة الآلية للمعطيات والتنبه لآثارها السلبية، بدأت خطط مكافحتها تحظى باهتمام متزايد من الحكومات و حتى العديد من المنظمات الدولية .

ومع أن الإجرام المعلوماتي لم يتخذ في الواقع الجزائري بعد و الواقع العربي كذلك الأبعاد التي اتخذها في الدول المتقدمة، إلا أن ذلك لا ينف ضرورة التصدي لبوادره كي لا يستفحل مع وتيرة النمو المتسارع الذي تشهده دول عربية عدة ومن بينها الجزائر في استخدام النظم المعلوماتية.

وتتمحور الإشكالية الأساسية التي يطرحها موضوع دراستنا في إبراز المشاكل القانونية الجديدة التي أفرزها ظهور المعلوماتية و تطبيقاتها المتعددة في نطاق القانون الجنائي. بمعنى البحث فيما إذا كانت النصوص القانونية القائمة كافية لمواجهة هذه الجرائم أم أن الأمر يستدعي استحداث قوانين أو نصوص خاصة قادرة على احتوائها و مراعاة طبيعتها و خصوصيتها.

لابد من الاعتراف أن الإجابة عن الإشكالية التي يطرحها موضوع الجريمة المعلوماتية مهمة تعترضها صعوبة منهجية كبرى مصدرها إتساع و تشعب الجوانب التي تتعلق بالمعلوماتية ، وهذا نظرا لما يتسم به هذا الموضوع من صبغة علمية غريبة على دارس القانون ، وذلك لاتصاله بجانب تقني فني يتمثل بالنظام المعلوماتي بشقيه المادي والمعنوي، فضلا عن قلة المراجع في المكتبة العربية حول الجرائم المعلوماتية، وكذلك ندرة التطبيقات القضائية في هذا المجال.

الفصل الأول: خصائص الجريمة في بيئة التجارة الالكترونية

تعتبر الجريمة في بيئة التجارة الالكترونية من الظواهر الحديثة وذلك لارتباطها بتكنولوجيا متطورة هي تكنولوجيا المعلومات. ونتيجة لحداثة هذه الجريمة فقد كانت هناك اتجاهات مختلفة في تعريفها كما اتسمت بمجموعة من الخصائص والسمات التي ميزتها عن غيرها من الجرائم الأخرى، كما أن هذه الجريمة جلبت معها طائفة جديدة من المجرمين اصطلح على تسميتهم بمجرمي المعلوماتية[1]. (نهلا عبد القادر المومني ،الجرائم المعلوماتية– ماجيستار في القانون الجنائي المعلوماتي– ، الطبعة الأولى، دار الثقافة للنشر والتوزيع، 2008م، ص45)

لهذا سوف نتناول في هذا الفصل ماهية الجريمة المعلوماتية من خلال مبحثين، الاول خصصناه لخصائص جرائم التجارة الالكترونية، أما الثاني السمات الخاصة للمجرم المعلوماتي

المبحث الأول :خصائص جرائم التجارة الالكترونية

نظرا لوقوع الجريمة المعلوماتية في غالبية الأحيان في بيئة المعالجة الآلية للبيانات ، حيث تكون المعلومات محل الاعتداء عبارة عن نبضات إلكترونية فإننا أمام ظاهرة إجرامية ذات طبيعة خاصة ذات صلة بما يعرف بالقانون الجنائي المعلوماتي. ووقوع هذه الجرائم في بيئة المعالجة الآلية للبيانات يعطيها لونا أو طابعا قانونيا خاصا ، يميزها بمجموعة من الخصائص ، بعضها قد يتطابق مع خصائص طوائف أخرى من الجرائم ، وبعضها الآخر يميزها عن الجرائم التقليدية لصعوبة كشف وإثبات الجرائم الأولى دون الثانية.(آمال قارة، المرجع السابق،ص24)

[1] **Éric A. CAPRIOLI, Transparence et sécurité des informations financières par voie électronique dans le règlement AMF après l'arrêté du 4 janvier 2007, Revue Communication Commerce électronique n° 6, Juin 2007, comm. 87**

وعلى ذلك فإننا سنقسم هذا المبحث إلى ثلاثة مطالب، الأول نتناول فيه خصائص الجرائم المعلوماتية، ، أما الثاني سنحاول فيه تحديد الطبيعة القانونية للجرائم المعلوماتية ، كما نتطرق في الثالث إلى صعوبات التصدي لهذه الجريمة.

المطلب الأول: خصائص الجرائم المعلوماتية

إن الجرائم المعلوماتية ذات خاصية منفردة حيث أن تلك الخاصية لا تتوافر في أي من الجرائم التقليدية سواء في أسلوبها أو في طريقة ارتكابها ، وتلك الخصائص نوردها فيما يلي:

الفرع الاول : الحاسب الآلي هو أداة ارتكاب الجريمة المعلوماتية:

يعتبر الحاسب الآلي الأداة الرئيسية التي تمكن الشخص من تنفيذ جريمته أيا كان نوعها ، بمعنى أن الحاسب الآلي هو الأداة الوحيدة لارتكاب أي جريمة من الجرائم المعلوماتية [1].(د/ عمروعيسى الفقى، الجرائم المعلوماتية، المكتب الجامعي الحديث،الإسكندرية،2006، ص85)

الفرع الثاني : الجريمة المعلوماتية ترتكب ضمن نظام المعالجة الآلية للمعطيات:

من خصائص الجريمة المعلوماتية أنها تقع أثناء المعالجة الآلية للبيانات والمعطيات الخاصة بالكومبيوتر ، ويمثل هذا النظام الشرط الأساسي الذي يتعين توافره حتى يمكن البحث في قيام أو عدم قيام أركان الجريمة المعلوماتية . ذلك أنه في حالة تخلف هذا الشرط تنتفي الجريمة المعلوماتية.(د/ خالد ممدوح إبراهيم، المرجع السابق، 2008، ص49)

الفرع الثالث : الجريمة المعلوماتية لا حدود جغرافية لها:

إن الجرائم المعلوماتية قد ترتكب عن طريق حاسب آلي في دولة ما ، في حين يتحقق الفعل الإجرامي في دولة أخرى ، فالجرائم المعلوماتية لا تحدها حدود ولا تعترف إبتداءا بعنصر المكان أو حدود الجغرافيا ، وتتميز بالتباعد الجغرافي بين الفاعل والمجني عليه ، ومن الوجهة التقنية بين الحاسوب أداة الجريمة ، وبين المعطيات أو البيانات محل الجريمة في نظام الحاسوب المستهدفة بالاعتداء ، هذا التباعد قد يكون ضمن الحدود الوطنية وقد يمتد خارج هذه

[1]

الحدود ليطال دولة أخرى.(يونس عرب،صور الجرائم الإلكترونية و اتجاهات تبويبها، بحث منشور على الموقع:www.arblaw.org)

الفرع الرابع : خطورة الجريمة المعلوماتية:

تتسم الجريمة المعلوماتية بالخطورة البالغة نظرا لأغراضها المتعددة ونظرا لحجم الخسائر الناجمة عنها قياسا بالجرائم التقليدية . ذلك أنها تمس الإنسان في فكره وحياته الخاصة ، وتمس المؤسسات في اقتصادها ، والبلاد في أمنها القومي والسياسي و الاقتصادي [1].(د/محمود أحمد عبابنة، المرجع السابق،ص32)

الفرع الخامس : أسلوب إرتكاب الجريمة المعلوماتية:

ذاتية الجرائم المعلوماتية تبرز بصورة أكثر وضوحا في أسلوب ارتكابها وطريقتها ، فإذا كانت الجرائم التقليدية تتطلب نوعا من المجهود العضلي الذي قد يكون في صورة ممارسة العنف ، فإن الجرائم المعلوماتية هي جرائم هادئة بطبيعتها لا تحتاج إلى العنف ، بل كل ما تحتاج إليه هو القدرة على التعامل مع جهاز الحاسوب بستوى تقني يوظف في ارتكاب الأفعال غير المشروعة.(نهلا عبد القادر المومني ،المرجع السابق، ص57و58)

الفرع السادس : خصوصية مجرمي المعلوماتية:

المجرم الذي يقترف الجريمة المعلوماتية يتسم بخصائص معينة تميزه عن المجرم الذي يقترف الجرائم التقليدية.فإذا كانت الجرائم التقليدية لا أثر فيها للمستوى العلمي والمعرفي للمجرم في عملية ارتكابها فإن الأمر يختلف بالنسبة للجرائم المعلوماتية فهي جرائم فنية تقنية في الغالب الأعم ، ومن يرتكبها عادة يكون من ذوي الاختصاص في مجال تقنية المعلومات ، أو على الأقل شخص لديه حد أدنى من المعرفة والقدرة على استعمال جهاز الحاسوب والتعامل مع شبكة الأنترنت.(نهلا عبد القادر المومني،نفس المرجع ، ص58و59)

---

[1] **Christophe CARON, Vers un droit pénal communautaire de la contrefaçon, Revue Communication Commerce électronique n° 6, Juin 2007, Repère 6**

المطلب الثاني : الطبيعة القانونية للجريمة المعلوماتية

يثور التساؤل بخصوص الوضع القانوني للمعلومة ، هل للمعلومات قيمة في ذاتها أم على العكس لها قيمة ما تتمثل في أنها مجموعة مستحدثة من القيم ، وبعيدا عن أساسها المادي فهل يمكن اعتبارها قيمة قابلة للاستئثار،إذ يمكن الاعتداء عليها بأي طريقة كانت ؛ ومن أجل ذلك انقسم الفقه إلى اتجاهين : الأول يرى أن المعلومة لها طبيعة من نوع خاص ، والثاني يرى أن المعلومة ما هي إلا مجموعة مستحدثة من القيم.(د/محمد علي العريان، الجرائم المعلوماتية، دار الجامعة الجديدة للنشر، الإسكندرية،2004م، ص49)

الفرع الاول : المعلومة لها طبيعة من نوع خاص:

يرى الفقه التقليدي أن للمعلومة طبيعة خاصة وذلك انطلاقا من حقيقة مسلم بها هي أن وصف القيمة يضفى على الأشياء المادية وحدها أي بمعنى آخر أن الأشياء التي توصف بالقيم هي تلك الأشياء القابلة للاستحواذ ، وبمفهوم المخالفة وباعتبار أن المعلومات لها طبيعة معنوية فلا يمكن والحال كذلك اعتبارها من قبيل القيم القابلة للاستحواذ عليها ؛ إلا في ضوء حقوق الملكية الفكرية .(د/محمد علي العريان،نفس المرجع ، ص49)

وقد جرت محكمة النقض الفرنسية قبل صدور قانون 1970م على الاستعانة بفكرة الخطأ لكي تعترف بالحق في احترام الحياة الخاصة ، ويبدوا أن هذا الحكم أقر بوجود الخطأ ليس على أساس المسؤولية التقصيرية وبذلك يكون قد أقر بوجود حق على المعلومات . (د/أحمد خليفة الملط ، الجرائم المعلوماتية، دراسة مقارنة، 2005م، ص125)

الفرع الثاني : المعلومات مجموعة مستحدثة من القيم

يرى الفقه الحديث أن المعلومات ما هي إلا مجموعة من القيم المستحدثة ويرجع الفضل في ذلك للأستاذين (Vivantو Catala) حيث يرى الأستاذ Catala أن المعلومة المستقلة عن دعامتها المادية تكون لها قيمة قابلة للاستحواذ على سند أن المعلومة تقوم وفقا لسعر السوق متى كانت

غير محضورة تجاريا وأنها تنتج بصرف النظر عن دعامتها المادية عن عمل من قدمها وأنها ترتبط بمؤلفها عن طريق علاقة قانونية تتمثل في علاقة المالك بالشيء الذي يملكه وهي تخص مؤلفها بسبب علاقة التبني التي تجمع بينهما. (د/ محمد علي العريان، المرجع السابق، ص50)

أما الأستاذ Vivant فيؤسس ذلك على حجتين : الأولى مستمدة من رأي Planiol و Ripert وهي أن فكرة الشيء أو القيمة لها صورة معنوية ، وأن نوع محل الحق يمكن أن ينتمي إلى قيمة معنوية ذات طابع اقتصادي وأن تكون جديرة بحماية القانون ،أما الحجة الثانية هي أن كل الأشياء المملوكة ملكية معنوية والتي يعترف بها القانون ، وترتكز على الاعتراف بأن للمعلومة قيمة ، عندما تكون من قبيل البراءات أو الرسومات أو النماذج أو التحصيلات الضرورية أو حق المؤلف[1].(د/ أحمد خليفة الملط ،نفس المرجع ، ص128)

والإنسان الذي يكشف ويقدم ويطلع الجماعة على شيء ما بصرف النظر عن الشكل او الفكرة ، فهو يقدم لهم معلومة بالمعنى الواسع ولكنها خاصة به ، ويجب أن تعامل هذه الأخيرة بوصفها قيمة وتصبح محلا للحق فلا توجد ملكية معنوية بدون الإقرار بالقيمة المعلوماتية.(د/ أحمد خليفة الملط ،نفس المرجع ، ص128)

إذن فان معنى ما تقدم اعتبار أن المعلومات مال قابل للتملك أو الاستغلال، على أساس قيمته الاقتصادية وليس على أساس كيانه المادي ، ولذلك فهو يستحق الحماية القانونية. ولما كانت البرامج في جوهرها معلومة معالجة بطريقة آليا ولها قيمة اقتصادية، فانه يجب معاملتها معاملة المال.(د/ محمد علي العريان، المرجع السابق، ص51)

المطلب الثالث : معوقات التصدي للجريمة المعلوماتية

إن الجرائم المعلوماتية تثير تحديات قانونية وعملية بالغة تقف عائقا أمام التصدي لها والوصول إلى مرتكبيها ، وتتمثل أهم هذه الصعوبات فيما يلي:

---

[1]**Éric A. CAPRIOLI, Mesures techniques de protection et d'information des droits d'auteur, Revue Revue Communication Commerce électronique n° 11, Novembre 2006, Etude 30**

الفرع الأول : صعوبة اكتشاف الجريمة المعلوماتية:

تتميز الجريمة المعلوماتية بصعوبة اكتشافها فإذا اكتشفت فإن ذلك يكون بمحض الصدفة عادة ، ويمكن رد الأسباب التي تقف وراء الصعوبة في اكتشاف الجريمة المعلوماتية إلى عدم ترك هذه الجريمة لأي أثر خارجي بصورة مرئية كما أن الجاني يمكنه ارتكاب هذه الجريمة في دول وقارات أخرى، كذلك فإن قدرة الجاني على تدمير دليل الإدانة في أقل من الثانية الواحدة يشكل عاملا إضافيا في صعوبة اكتشاف هذا النوع من الجرائم ، فالجرائم المعلوماتية في أكثر صورها خفية لا يلحظها المجني عليه أو لا يدري حتى بوقوعها. (نهلا عبد القادر المومني،المرجع السابق، ص53و54)

الفرع الثاني : صعوبة إثبات الجريمة المعلوماتية:

إكتشاف الجريمة المعلوماتية أمر ليس بالسهل ولكن حتى في حال اكتشاف وقوع هذه الجريمة والإبلاغ عنها فإن إثباتها أمر يحيط به الكثير من الصعاب ويرجع ذلك إلى عدة أمور منها: (د/خالد ممدوح إبراهيم،المرجع السابق، ص45و46)

1-أنها كجريمة لا تترك أية آثار مادية بعد ارتكابها ، فهي جريمة تقع في بيئة إلكترونية.

2- صعوبة الاحتفاظ الفني بدليل الجريمة المعلوماتية إذ يستطيع المجرم المعلوماتي في أقل من ثانية أن يمحو البيانات المخزنة بجهاز الكومبيوتر.

3- تحتاج إلى خبرة فنية ويصعب على المحقق التقليدي التعامل معها حيث تتطلب الجرائم المعلوماتية إلمام خاص بتقنيات الكومبيوتر ونظم المعلومات.

الفرع الثالث : صعوبة الوصول إلى الجاني الحقيقي:

في أغلب الأحيان يدخل الجاني إلى الانترنت عن طريق مقاهي الانترنت الأمر الذي يصعب التعرف عليه وتحديد موقع إتصاله، كما قد يكون الجاني مقيم بالخارج مما يصعب إلحاق العقوبة به.(عمروعيسى الفقى ،المرجع السابق ،ص91)

الفرع الرابع : الطبيعة الدولية للجريمة المعلوماتية و تداعياتها:

طالما أن الجريمة المعلوماتية ذات طبيعة دولية فإن ذلك يؤدي إلى تشتيت جهود التحري والتنسيق الدولي لتعقب مثل هذه الجرائم ،فهذه الجرائم هي صورة صادقة من صور العولمة.(د/ محمود صالح العادلي ، الجرائم المعلوماتية،ص7)

فالجريمة المعلوماتية تخترق الحدود بدون حسيب أو رقيب الأمر الذي يثير التساؤل حول تحديد القانون الواجب التطبيق على هذه الجريمة ، فهل تطبق قوانين الدولة التي ارتكب فيها الجرم أو الدولة التي وقع فيها النشاط الإجرامي ، أي النتيجة؟ (د/ نعيم مغبغب، حماية برامج الكومبيوتر،منشورات الحلبي الحقوقية،الطبعة الأولى،2006م،ص219)

الفرع الخامس : قلة الإبلاغ عن وقوع الجريمة المعلوماتية:

لا يتم في الغالب الأعم الإبلاغ عن الجرائم المعلوماتية إما لعدم اكتشاف الضحية لها، وإما خشيته من التشهير، لذا نجد أن معظم الجرائم المعلوماتية تم اكتشافها بالمصادفة ، بل وبعد وقت طويل من ارتكابها زد على ذلك أن الجرائم التي لم تكتشف هي أكثر بكثير من تلك التي كشف الستار عنها ، وهو ما يزيد من عدم التعرف على مرتكبي هذه الجرائم.(د/ خالد ممدوح إبراهيم ، المرجع السابق، ص51)

المبحث الثاني : السمات الخاصة للمجرم المعلوماتي

إن أية ظاهرة إجرامية ، أو أي نمط إجرامي مستحدث له من الخصائص ما قد يميزه عن غيره، كذلك فإن مرتكبي أي نمط إجرامي لهم من السمات ما يميزهم عن غيرهم. لهذا سوف نتناول في هذا المطلب دراسة السمات الخاصة لشخصية المجرم المعلوماتي على النحو التالي:

المطلب الأول : خصائص المجرم المعلوماتي

تتوافر لدى الجناة مرتكبي الجرائم المعلوماتية أو معظمهم مجموعة من الخصائص التي تميزهم عن غيرهم من الجناة أو المتورطين في أشكال الإنحراف و الإجرام الأخرى،ولعل من أبرز هذه الخصائص ما يلي:

أولا-السن:

تتراوح أعمار مقترفي جرائم المعلوماتية عادة مابين 18و46 سنة والمتوسط العمري لهم 25 سنة. (محمد عبد الله أبو بكر سلامة،المرجع السابق، ص98)

ثانيا- المهارة والخبرة في مجال نظم المعلومات:

يتمتع مجرمو المعلوماتية بقدر لا يستهان به من المهارة والخبرة بتقنيات الحاسوب والانترنت ، بل إن بعض مرتكبي هذه الجرائم من المتخصصين في مجال معالجة المعلومات آليا . فالمهارة والخبرة هما اللذان يحددان الأسلوب الذي تتم به جريمة التعدي.(نهلا عبد القادرالمومني،المرجع السابق، ص77)

ثالثا – الذكاء:

يتميز المجرم المعلوماتي غالبا بالذكاء ، فالإجرام المعلوماتي هو إجرام الأذكياء بالمقارنة بالإجرام التقليدي الذي يميل إلى العنف، فالمجرم المعلوماتي يستخدم مقدرته العقلية ولا يلجأ إلى إستخدام العنف أو الإتلاف المادي بل يحاول أن يحقق أهدافه بهدوء.(نهلا المومني،نفس المرجع ، ص77)

كما تتجلى صفة الذكاء للمجرم المعلوماتي في اكتشافه الثغرات الأمنية للبرامج الموضوعة بمعرفة المتخصصين ، بالرغم من المحاولات المستمرة لتحديث أنظمة الدفاع الأمني لهذه البرامج.(إيهاب فوزي السقا، الحماية الجنائية والأمنية لبطاقات الإئتمان، دار الجامعة الجديدة ، الإسكندرية، 2007، ص132)

رابعا- الإلمام بمسرح الجريمة

المجرم المعلوماتي في العادة يمهد لإرتكاب جريمته، بالتعرف على المحيط الذي يريد ارتكاب جريمته فيه للتعرف على كافة الظروف التي تحيط بالهدف المراد الوصول إليه؛وذلك حتى لا يفاجئ بأمور غير متوقعة من شأنها إفشال مخططاته والكشف عنها.(إيهاب فوزي السقا ،نفس المرجع ، ص132)

خامسا – المجرم المعلوماتي إنسان إجتماعي:

المجرم المعلوماتي هو عادة إنسان إجتماعي قادر على التكيف في بيئته الاجتماعية بل إن بعضهم يتمتع بثقة كبيرة في مجال عمله ، فهو إنسان مرتفع الذكاء مما يساعده على عملية التكيف في المجتمع. بل إن خطورته الإجرامية قد تزداد إذا زاد تكيفه الاجتماعي مع توافر الشخصية الإجرامية لديه (نهلا عبد القادر المومني،المرجع السابق، ص79)

سادسا–المجرم المعلوماتي يبرر ارتكاب جريمته:

يوجد شعور لدى مرتكب فعل الإجرام المعلوماتي أن ما يقوم به لا يدخل في عداد الجرائم، حيث يفرق مرتكبو هذه الجرائم بين الإضرار بالأشخاص الأمر الذي يعدونه غاية في اللاخلاقية وبين الإضرار بمؤسسة أو جهة في استطاعتها اقتصاديا تحمل نتائج تلاعبهم. (نهلا عبد القادر المومني، نفس المرجع ، ص78)

سابعا– الحرص الشديد وخشية الضبط:

يتصف مجرمو المعلوماتية بالخوف من كشف جرائمهم وافتضاح أمرهم ، وبالرغم أن هذه الخشية تصاحب المجرمين على اختلاف أنماطهم إلا أنها تميز مجرمي المعلوماتية بصفة خاصة، وهذه الخشية لدى مجرمي المعلوماتية من اكتشاف أفعالهم مردها إنتماؤهم في الغالب الأعم إلى وسط اجتماعي متميز، سواء من حيث التعليم أو الثقافة أو المستوى المهني وطبيعة العمل. (نهلا عبد القادر المومني،نفس المرجع، ص79و80)

المطلب الثاني : أنماط المجرم المعلوماتي

إن التطور والتغير السريع في أنماط الجريمة المعلوماتية وصورها ، شكل صعوبة في وضع تصنيف ثابت لطوائف مجرمي المعلوماتية ، ولكن يمكن لنا وفقا لما توصلت له الدراسات والأبحاث التي تناولت مجرمي المعلوماتية أن نبين فيما يلي أهم الفئات لمرتكبي هذه الجرائم.

(نهلا عبد القادر المومني،نفس المرجع ، 77)

الفئة الأولى: القراصنة les pirates

هناك نوعان من القراصنة:

النوع الأول: القراصنة الهواة (الهاكرز) hackers

هذا القسم من القراصنة الذي اصطلح على تسميتهم بالهاكرز يرون في اختراق الأنظمة المعلوماتية تحديا لقدراتهم الذاتية ، وهذه الطائفة غالبا ما تكون من هواة الحاسوب ؛ولا تتوافر لديهم في الغالب دوافع حاقدة أو تخريبية وإنما ينطلقون من دوافع التعدي وإثبات المقدرة.(نهلا عبد القادر المومني،المرجع السابق، ص83)

والسمة الغالبة على أعضاء هذه الطائفة صغر السن وقلة الخبرة وعدم التمييز بين الأنظمة محل الاختراق ، ولكن رغم هذه السمات فقد تمكن المجرمون من هذه الطائفة من اختراق مختلف أنواع نظم الكومبيوتر التابعة لشركات المالية والمؤسسات الحكومية. كما أن السمة المميزة لهذه الطائفة أنهم يبادلون فيما بينهم المعلومات و التقنيات المتبعة لاختراق النظم بواسطة الرسائل أو عن طريق عقد اجتماعات. وقد ساهم العديد من أعضاء هذه الطائفة في تطوير نظم الأمن في مختلف المؤسسات ، حتى أن العديد من الجهات تستعين بخبراتهم في أحيان كثيرة في فحص وتدقيق مستوى أمن نظم الكومبيوتر والمعلومات.(بوكثير خالد،الجرائم المعلوماتية ، مذكرة تخرج ، 2005–2006، ص8)

النوع الثاني: القراصنة المحترفون(الكراكرز) crackers

تتميز هذه الطائفة بسعة الخبرة و الإدراك الواسع للمهارات التقنية ، كما تتميز بالتنظيم والتخطيط للأنشطة التي ترتكب من طرف أفرادها وهو ما يجعلها في غاية الخطورة. حيث تهدف اعتداءاتهم بالأساس إلى تحقيق الكسب المادي لهم أو الجهات التي كلفتهم لارتكاب هذه الجرائم .(بوكثير خالد، نفس المرجع،ص8)

ومن مميزات هذه الطائفة أن أفرادها يتميزون بالتكتم عكس الفئة الأولى فلا يتبادلون المعلومات المتعلقة بأنشطتهم ، بل يطورون معارفهم الخاصة ويحاولون ما أمكن عدم كشف طرقهم التقنية لارتكاب جرائمهم ، وحول الأعمار الغالبة على هذه الطائفة فإن الدراسات تشير إلى أنها تتراوح ما بين 25و40 عاما.(بوكثيرخالد،نفس المرجع ،ص8)

الفئة الثالثة: الموظفون العاملون في مجال الأنظمة المعلوماتية

بحكم طبيعة عمل هؤلاء الموظفين ونظرا لأن النظام المعلوماتي هو مجال عملهم الأساسي ، ونظرا للمهارات والمعرفة التقنية التي يتمتعون بها فإنهم يقترفون بعض الجرائم المعلوماتية التي من الممكن أن تحقق أهدافهم الشخصية وأهمها الكسب المادي. كما أن هناك فئة من الموظفين الحاقدين على عملهم تحركهم الرغبة بالانتقام والثأر كأثر لتصرف صاحب العمل معهم. وهذه الفئة يذهب البعض إلى تسميتها بفئة مجرمي المعلوماتية الحاقدين.(نهلا عبد القادرالمومني، المرجع السابق، ص85)

الفئة الرابعة: مجرمو المعلوماتية المتطرفون

تتألف هذه الفئة من الجماعات الإرهابية أو المتطرفة التي تتكون من مجموعة من الأشخاص لديهم معتقدات و أفكار اجتماعية أو سياسية أو دينية ويرغبون في فرض هذه المعتقدات باللجوء إلى النشاط الإجرامي. فهذه الجماعات تدافع عن قضية أو معتقد معين ولا تهدف إبتداءا إلى تحقيق الربح المادي.(نهلا عبد القادر المومني ،نفس المرجع ، ص85 و86)

الفئة الخامسة: مجرمو المعلوماتية في إطار الجريمة المنظمة

إن الجرائم المعلوماتية تشكل عامل جذب كبير لهذه المنظمات الإجرامية فبالإضافة إلى الأرباح المادية المرتفعة التي تنتج من هذه الجرائم فإن صعوبة الكشف عنها وصعوبة إثباتها جعل منها مادة إجرامية دسمة تغري هذه الجماعات باقترافها.(نهلا عبد القادر المومني، المرجع السابق،ص88)

فلقد وجدت هذه المنظمات في شبكة الانترنت وسيلة لا تضاهى للقيام بعمليات غسيل الأموال وتدعيم تجارة الرقيق الأبيض وتجارة الأعضاء البشرية عبر إنشاء مواقع خاصة. وهذه التقنيات الحديثة تتناسب مع طبيعة النشاطات الإجرامية لجماعات الجريمة المنظمة التي تعد من الجرائم العابرة للحدود.(نهلا عبد القادر المومني، المرجع السابق ، ص88)

الفئة السادسة: الجواسيس

هؤلاء مهمتهم إستخبارية، فهي تقتصر على جمع المعلومات لمصلحة دولهم ، أو لمصلحة بعض الأشخاص ، أو الشركات التي تتنافس فيما بينها ومن مقتضيات عملهم أن لا يتركوا دليلا على عملهم، لذلك فهم يتمتعون بقدرة عالية على التعامل مع الحاسب الآلي إلى جانب قدرتهم على طمس الأدلة التي تتخلف عن جرائمهم. (محمد حماد مرهج الهيتي، جرائم الحاسوب ، دار المناهج ، عمان ، 2005، ص137)

المطلب الثاني : الدافع إلى ارتكاب الجرائم المعلوماتية

إن أهم ما يميز الإجرام المعلوماتي عن الإجرام التقليدي هو وجود تقنية المعلومات التي تصبغ نموذج الجريمة المعلوماتية .(د/ محمد علي العريان المرجع السابق، ص65)

حيث أن لهذه الجريمة عدة دوافع على ارتكابها فبعضها يرجع إلى دافع شخصي ومنها ما يرجع إلى دافع خارجي ومنها ما يكون خاص بالمنشأة ، وكل هذه الدوافع قد يكون مصدرها هو الرغبة الإجرامية.(د/ أحمد خليفة الملط ، المرجع السابق،ص99)

أولا- الدوافع الشخصية:

يمكن رد الدوافع الشخصية لدى مرتكب الجرائم المعلوماتية إلى دوافع مالية ودوافع ذهنية أو نمطية وهما أهم الدوافع لدى المجرم المعلوماتي في ارتكاب مثل هذه الجرائم. (د/ أحمد خليفة الملط ،نفس المرجع ، ص99)

الدوافع المادية:

أحيانا يكون الهدف من ارتكاب جرائم الكومبيوتر للحصول على ربح مالي عن طريق المساومة على البرامج والمعلومات المتحصلة بطريق الاختلاس من جهاز الكومبيوتر. (د/محمد أمين الرومي، جرائم الكومبيوتر و الانترنت، دار المطبوعات الجامعية،2004م، ص24)

ومثال ذلك واقعة استيلاء مبرمج بإحدى الشركات الألمانية على إثنين وعشرين شريط خاص بمعلومات هامة عن عملاء وانتاج الشركة وقام بتهديد شركته بدفع مبلغ 200.000 دولار وإلا

سيتم بيعها إلى الشركات المنافسة ، ورأت الشركة دفع المبلغ تجنبا للخسائر الناتجة في حالة بيع الشرائط للمنافسين.(د/ أحمد خليفة الملط، المرجع السابق،ص99)

وهناك فئة من مرتكبي الجرائم المعلوماتية يرجع ارتكابهم لها لما تحققه من ثراء فاحش والدليل على ذلك ما حدث في فرنسا سنة 1986م حيث كان العائد من ارتكاب جناية سرقة مع حمل السلاح هو سبعون ألف فرنك في حين أن جريمة غش في مجال المعالجة الآلية للمعلومات حصل منها الجاني على مائتي ن وسبعون ألف فرنك أي ما يعادل أكثر من ثمانية وثلاثون مرة.(د/أحمد خليفة الملط ،نفس المرجع ، ص99)

الدوافع الذهنية أو النمطية:

غالبا ما يرتكب المبرمج جرائم الكومبيوتر نتيجة إحساسه بالقوة والرغبة في إثبات الذات وقدرته على اقتحام النظام وتحقيق انتصار على تقنية الأنظمة المعلوماتية دون أن يكون لهم نوايا آثمة .(د/محمد علي العريان ، المرجع السابق، ص63)

ويرجع ذلك إلى وجود عجز في التقنية التي تترك الفرصة لمشيدي برامج النظام المعلوماتي لارتكاب تلك الجرائم ، مثال ذلك في فرنسا نشر في جريدة الاكسبريس الفرنسية في سبتمبر سنة 1983م تحت عنوان " ميلاد نزعة" قيام عامل طلاء يدعى Roland Lava بجريمة سطو وذلك عندما توجه إلى أحد البنوك لإيداع شيك وشاهد في تلك اللحظة فصل الموزع الآلي للنقود عند قيام مستخدم الصيانة باستخراج نقود البنك من الآلة " عند الطلب " عن طريق استخدام بطاقة خاصة وقد أحدث هذا تصدعا في رأسه وحياته فقام بالتدريب على الحاسب الآلي لمدة عامين وقام بعد ذلك بالسطو على صانع الموزعات الآلية وبفضل الآلة المسروقة تمكن من سحب النقود وألقي عليه القبض قبل أن يستفيد من نزعته المستحدثة ونسب إليه جريمة سرقة الآلة.(د/ محمد علي العريان ،نفس المرجع ، ص63)

ثانيا- الدوافع الخارجية:

فالإنسان بطبيعته يتأثر ويستسلم للمؤثرات الخارجية أو أن يحدث نتيجة سلوكه المخادع لدوافع عديدة لارتكابه تلك الجرائم مثال ذلك: دافع الانتقام الذي أدى بشاب محاسب أن يتلاعب في

برامج الكومبيوتر الخاصة بالشركة التي يعمل بها . حيث برمجها على أن تختفي كل البيانات الخاصة بديون الشركة بعد مضي ستة أشهر من تركه للعمل حدث بالفعل ما أراد واختفت البيانات الخاصة بديون الشركة نهائيا من جهاز الكومبيوتر. (د/ محمد أمين الرومي، المرجع السابق، ص25)

كما قد يكون دافع التعاون و التواطئ على الأضرار، فهذا النوع كثير التكرار في الجرائم المعلوماتية وغالبا ما يحدث من متخصص في الأنظمة المعلوماتية يقوم بالجانب الفني من المشروع الإجرامي وآخر من المحيط أو خارج المؤسسة المجني عليها لتغطية عمليات التلاعب و تمويل المكاسب المادية إليه وعادة ما يمارسون التلصص على الأنظمة وتبادل المعلومات بصفة منظمة حول أنشطتهم .(د/محمد أمين الرومي، نفس المرجع، ص26)

الفصل الثاني

بعض الجوانب الإجرائية لجرائم التجارة الالكترونية

المبحث الأول : مرحلة ماقبل المحاكمة

يحتاج موضوع الجوانب الإجرائية لجرائم التجارة الإلكترونية إلى فقه متميز بتميز طريقة ارتكاب جرائمه فقه يتعامل من منطلق التطورات التقنية و المتقدمة.....، و لعل أهمية دراسة هذا الجانب لا تكمن في مجرد البحث في كيفية ارتكاب الجريمة و معرفة الفاعل أهميته تتضح من خلال استجلاء الخطورة المتعلقة بالتفاوت في الوعي و التمكن من تكنولوجيا المعلومات و المرقمة من الدول عامة و أطراف العلاقات التعاقدية ثانيا بالأخص أن أغلب المتعاملين في مجال التجارة الإلكترونية هم مستهلكون ضعيفوا التمكن من آليات الرقمية و تقنياتها بالمقارنة مع الطرف القوي أي المحترف[1].

على قدر قدرة (كفاءة) الجوانب الإجرائية في التصدي لجرائم هذه التجارة. تظهر كفاءة الدول في الانخراط في منظومة الاقتصاد الرقمي و الانتماء إلى العالم الافتراضي فليس تكويني بالطبع مجرد التجريم من الناحية الموضوعية بأن إغفال تطوير جانب الإجراءات سيصيب الأمر بصفة الجمود[2]. و هذا الضعف في مكافحة الجريمة و هو حتى سيهدم عقوبات الإدانة ليشيد هيكل البراءة فتصبح النتيجة تبرئة المجرم حال لزوم معاقبته[3].

و جرائم المعلوماتية عموما و جرائم التجارة الإلكترونية بالخصوص جعلت المشرع أمام تحدي نشوء مراكز قانونية جديدة و مشكلة حمايتها ضد التهديد التي تحمله ذات الآلية التي أنشأ بها. و قد أفاد موضوع القاعدة القانونية في المعلوماتية وجود طائفة من الجرائم التقليدية المرتكبة بهذه الآلية لها وجود مسبق و أي سوابق قضائية في القاعدة الموضوعية (جرائم النسب، التجارة، الدعارة، التزوير...)، و أفادت كذلك جرائم لم يكن لها وجود قبل ذلك و لا سوابق في علم القانون ككل و القانون الجنائي على وجه الخصوص الأمر الذي يلزم تدخل المشرع لأول مرة على المستوى الموضوعي و الإجرامي بما يرضي ضمير العدالة و يحقق الحماية للحقوق و الحريات.[4]

---

[1] **Éric A. CAPRIOLI, Mesures techniques de protection et d'information des droits d'auteur, Revue Revue Communication Commerce électronique n° 11, Novembre 2006, Etude 30**

[2] - عمر محمد أبوبكر بن يونس ، مرجع سابق ، ص785.
[3] - عمر محمد أبوبكر بن يونس ، مرجع سابق ، ص786.
[4] - عمر محمد أبوبكر بن يونس ، مرجع سابق ، ص786.

الجانـــــب الموضوعـــــي:

و إذا كان الجانب الموضوعي أو القاعدة الموضوعية لجرائم التجارة الإلكترونية ذات تمديد شمل مجموعة من الجرائم المرتبطة بطبيعة هذه التعاملات فإن الوضع يختلف بالنسبة للإجراءات الجنائية المفترض اتخاذها اتجاه جرائم التجارة الإلكترونية هو أمر كما يصفه البعض[1] يمتد ليشمل طائفة من الاستفسارات التي جعلت من مثل هذه الجرائم محلا للبحث عن أسلوب أو آليات من الإجراءات الموازية التي يمكن اعتمادها سعيا وراء التعامل الجنائي مع هذه الظاهرة التقنية الحديثة في الوقت الذي يلزم فيه حماية المستهلك و المتعامل على سواء من الاعتداء على مراكزهم في إطار هذه المعاملات التجارية الحديثة، و يتجاوز جانب الإجراءات إلى مشكل طرق الإثبات الجنائي حيث الدليل في عقود حيث الأسلوب التقليدي في البحث عن الأدلة أو في الأدلة ذاتها فإن الدفع في بطلانها لعدم توافقها مع التقنية الحديثة هو دفع جوهري[2].

تبعا لخصوصية تعاملات التجارة الالكترونية فان هذه الخصوصية تنسحب على تلك الإجراءات المقررة أو التي تنبغي أن تعتمد أثناء التحقيق أو أثناء....

المطلب الأول: المشكلات المتعلقة بسلطات الاستدلال:

شان الجريمة المعلوماتية كباقي الجرائم الأخرى من حيث المراحل التي تمر بها فيما تتعلق بالاستدلال والتحقيق بالرغم من كبر الصعوبات التي تعترضها بين المرحلتين تبعا لخصوصية الجرائم الواقعة على التجارة الالكترونية فيها.

الفرع الأول : الامتناع عن الإبـــــلاغ:

حرصا على السمعة التي تكتسبها الشركات من خلال تعاملاتها, فإنها تتخوف وعادة تمتنع المؤسسات عن التبليغ عن أي سطو يقع على أجهزتها فمثلا تحرص البنوك على عدم المساس بالثقة المكتسبة من قبل عملائها وتدرك مدى الآثار السلبية لفقدان تلك الثقة أو ضياعها من جراء شيوع الاختراق والسطو على هذه البرامج طبعا خشية سحب ودائعهم واستثماراتهم، ومثل ذلك يقال عن المواقع أو المتاجر الافتراضية (... ملتقى انعكاس ثورة المعلومات)

ولعل الصعوبة التي تواجه أجهزة الأمن والمحققين هي كون أن مثل تلك الاعتداءات والجرائم لا تصل إلى علمهم إما للسبب التي سبق بيانه أو لأنها أصلا (أي المؤسسات أو الشركات) لم يبلغ أصلا إلى علمها ، هذا ما يدعو سلطات الأمن في جرائم التجارة الالكترونية أن تصدر

---

[1] - عمر محمد أبوبكر بن يونس ، مرجع سابق ، ص787.

[2] - عمر محمد أبوبكر بن يونس ، مرجع سابق ، ص787.

ميدانيا حركة المبادلات التجارية عن طريق جمع المعلومات السرية عن حركة السوق وتداول الأموال، وكل ما يرتبط بمؤسسات الجريمة[1]، ويكون ذلك عن طريق:

ضبط شخص بحوزته بطاقات مزورة يفيد وقوع.

ورود بلاغ إلى سلطات الضبط أو التحقيق.

يفيد وقوع تلاعب أو اعتداء في صورة عجز مالي في حسابات مؤسسة أو تغيرات في الودائع أو ضياع مركز قانوني.

توافر معلومات عن وقوع عمليات اعتراض أو قرصنة معلوماتية.

تلقي سلطات الضبط أو التحقيق معلومات عن ممارسة الأنشطة الموصوفة بأنها جرائم تجارة الكترونية في مكان معين.[2]

توافر معلومات عن بث فيروسات تخرب نظام المعالجة أو تعرقل نشاط الموقع و تبطئ خدماته.

هذه الجريمة تفرض تحديا أمام سلطات الشرطة القضائية يتعلق أساسا بمدى قدرة الرصد الأمني و كفاءة أجهزة الرقابة المالية في الدولة [3] بما يجعل السلطات مضطرة إلى اتخاذ تدابير سابقة متمثلة في:[4]

تعليم رجال الأمن مبادئ المعلوماتية و التمكن من ميدان تقنيات المعاملات التجارية الالكترونية للتوصل إلى تحديد العناصر المكونة للسلوك الإجرامي.

إنشاء وحدة خاصة بمثل هذه الجرائم على شاكلة "الشرطة العلمية" تكون متخصصة و مؤهلة للتحقيق في الجرائم المتعلقة بالتعاملات المصرفية و الشركات التجارية الافتراضية (البنوك التجارية، المؤسسات المالية، الشركات التجارية) مراكز المعلوماتية، مراكز التحويلات المالية.

فرض تغطية أمنية على ما سبق من أماكن دون المساس بحقوق الخصوصية.

إبقاء أفراد الضبطية القضائية عل صلة بآخر التحديثات في مجال المعلوماتية.

رصد حركة المشبوهين في مجال جرائم التجارة الالكترونية على وجه خاص و مجري المعلوماتية.

---

[1] - فقد يكون أحد عينات الاستدلال صغار الموظفين و ذو القدرات الفنية الذين على صلة بأسرار و برامج المعلوماتية للمؤسسات المالية و التجارية. عبد الفتاح بيومي حجازي ، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت ، مرجع سابق ، ص 110.

[2] - عبد الفتاح بيومي حجازي ، الدليل الجنائي في جرائم التزوير والإنترنت ، مرجع سابق ، ص 70.

[3]- **Éric A. CAPRIOLI, Mesures techniques de protection et d'information des droits d'auteur,** Revue Revue **Communication Commerce électronique n° 11, Novembre 2006, Etude 30**

[4] - عبد الفتاح بيومي حجازي ، الدليل الجنائي في جرائم التزوير والإنترنت ، مرجع سابق ، ص 72- 73، عبد الفتاح بيومي حجازي ، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت ، مرجع سابق ، ص 113.

رصد قائمة لمجرمي الإجرام المعلوماتي (التزوير، التحويلات، غسيل الأموال) كعناصر استرشادية و كشفية لتتبع و اقتفاء أثر نظائرهم أثناء التحقيقات للحصول على أدلة موصلة أو كاشفة لوجوه الحقيقة في الدعوى الجنائية على التنسيق الذي استحدثه الصين حيث كونت شرطة متخصصة لمتابعة الاختراقات الالكترونية عندما أنشأ أحد أقاليمها أول وحدة بوليسية متخصصة لمراقبة استخدام شبكة الانترنيت[1].

و قد اهتمت الأنتربول كذلك بهذا النمط من الجرائم المستحدثة لتعزز بنشاطها الحماية الجنائية للتجارة الالكترونية بعدما أنشأت الأنتربول فرقة خاصة بمكافحة جرائم المعلوماتية بالتعاون مع فرق مكافحة الجريمة المعلوماتية في دول الاتحاد الأوروبي و الولايات المتحدة الأمريكية و استراليا في إطار عمليات الأساليب التقنية للكشف عن مثل هذه الجرائم و تعزيز الإجراءات الأمنية و تبادل الخبرات في هذا الميدان [2] و بخصوص مسألة الإبلاغ فإنها تشكل إشكالا لدى البعض و أفضل من نظمها في نظرنا هو، **اجتهادات بعض المشروعين في مسألة الإبلاغ:**

كان المشرع في دولة الإمارات العربية المتحدة حازما في مسألة الإبلاغ و هذا مذهب نؤيده نظرا لدرجة الخطورة الإجرامية و الشخصية المؤثمة في هذا الصنف من الجرائم حيث جعل الإبلاغ عن الجرائم ملزما كقاعدة عامة و يقع تحت طائلة المساءلة الجزائية كل من يخالف ذلك و هو منطوق المادة 37 من قانون الإجراءات الجزائية الاتحادي رقم 35/ 1992 حيث جعلت لزاما على كل من علم بوقوع جريمة مما يجوز للنيابة العامة رفع الدعوى عنها بغير شكوى أو طلب، أن يبلغ النيابة العامة أو أحد مأوى الضبط القضائي عنها.

و نصت المادة 38 من ذات القانون على أنه يجب على كل من علم من الموظفين العموميين أو المكلفين بخدمة عامة أثناء تأدية عمله جريمة من الجرائم التي يجوز للنيابة العامة رفع الدعوى عنها بغير شكوى أو طلب أن يبلغ فورا النيابة العامة أو أقرب مأوى الضبط القضائي.

و رتب المشرع على الإخلال بهذا الواجب عقوبة جنائية أقرتها المادة 272/ 2 من قانون العقوبات الاتحادي على أنه " يعاقب بالغرامة كل موظف غير مكلف بالبحث عن الجرائم أو ضبطها أهمل أو أرجأ إبلاغ السلطة المختصة بجريمة علم بها في أثناء تأديته وظيفته، و لا عقاب إذا كان رفع الدعوى معلقا على شكوى:

و إسقاطا على نوع الجرائم التي نحن بصدد دراستها فإن مؤدي هذه النصوص أنه المسؤولية الجنائية تطال المواطن العادي كما تطال الموظف في شركات القطاع الخاص و العام لامتناعهم

---

[1] - عبد الفتاح بيومي حجازي ، الدليل الجنائي في جرائم التزوير والإنترنت ، مرجع سابق ، ص 76، عبد الفتاح بيومي حجازي ، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت ، مرجع سابق ، ص 117.

[2] - عبد الفتاح بيومي حجازي ، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت ، مرجع سابق ، ص 117، عبد الفتاح بيومي حجازي ، الدليل الجنائي في جرائم التزوير والإنترنت ، مرجع سابق ، ص 76.

عن الإبلاغ متى انتهى إلى علمهم وقوع جرائم من هذا الصنف أي لها علاقة بجرائم التعاملات التجارية الالكترونية[1]، و هذا ما يجعل البعض يرى أنه إجراء يصب في مصلحة الدعوى الجنائية و إمكانية استجماع الأدلة بخصوص جرائم التجارة الالكترونية على وجه الخصوص وجرائم المعلوماتية عموما.[2]

الفرع الثاني : صعوبات خبرة سلطات الاستبدال والتحقيق:

مسألة البحث والتحقيق في جرائم التجارة الالكترونية مسالة في غاية التعقيد ومرجع ذلك تلك المرونة التي تطبع المعاملات التجارية بأول درجة حيث العقود التجارية وشروطها محل تتراصي الأطراف في الإنشاء والإلغاء أولا وثانيا بطبيعة المعاملة التي تتم بها هذه التجارة والآلية الالكترونية هي وسائل أو آليات متحدثة، يجعل عامل الجد فيها سلطات التحقيق والاستدلال أمام تحديات لم يكونوا قد تعودوا عليها من قبل بالنظر لاعتبارات التكوين والتدريب العلمي والخبرة التي يتمتع بها جهاز الضبطية القضائية وسلطات التحقيق الجنائي والحكم فالخلقية القانونية والخبرة التقليدية غير كافيتان للإحاطة بهذا النمط من الجرائم الفنية والسلوكيات الجرمية التقنية وبخاصة أن هؤلاء القائمين على البحث الجنائي والتحقيق فيه يواجهن نوع جد متخلف من المجرمين حيث الذكاء اكبر خاصية في سلوكاتهم الإجرامية زد على ذلك الإغراء المادي المعتبر والتي يفوق نسبة الأرباح المضاعفة التي توفرها التقنية الالكترونية في المجال التجاري والأجهزة العدالة الجنائية الممثلة في سلطات الاتهام والتحقيق الجنائي هذا النقص في الخبرة لذا جهاز الضبطية القضائية والملاحظ من قبل الفقد الجنائي يؤثر على الحد من هذه الظاهرة الاجرامية فالمعلوم أن أجهزة العدالة المقاومة لهذه الجرائم مرتبط ة بهذه التقنية تبدأ في التكوين عقب ظهور الأخيرة مما يعني أن وقت انتشار الجريمة هو أسرع من وقت التصدي لها فجرائم التجارة الالكترونية هي تسير بسرعة توازي سرعة التقنية حيث الإجرام والمعلوماتية ظاهرتان متلازمتان للأسف وأسف ثاني أن الحركة التشريعية والجهاز المخول بالبحث والتحقيق فيها والاستدلال عليها لا يسير بذات معدل التسارع.[3]

يعزر الدعوة إلى وجود سلطات الأمن عموما وأجهزة التحقيق والاستدلال والادعاء والحكم في هذه الجرائم هو تلك المفردات التي هي أدوات الجريمة في مجال التجارة الاليكترونية عموما وفي نفس الوقت هي مصطلحات حكر على الجناة ومجرمي المعلوماتية فهم بحق كما يصفون

---

[1] - و هذا إجراء سنه المشرع يتناسب و طبيعة النشاطات الالكترونية التجارية في تلك الدولة حيث هي أكبر المناطق التجارية الحرة و أنظمتها الحكومية و غير الحكومية تعتمد في أنشطتها على تقنية المعلوماتية.

[2] - عبد الفتاح بيومي حجازي ، الدليل الجنائي في جرائم التزوير والإنترنت ، مرجع سابق ، ص 79 – 80 ، عبد الفتاح بيومي حجازي ، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت ، مرجع سابق ، ص 119 – 120 .

[3] - عبد الفتاح بيومي حجازي ، الدليل الجنائي في جرائم التزوير والإنترنت ، مرجع سابق ، ص 81، عبد الفتاح بيومي حجازي ، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت ، مرجع سابق ، ص 122.

أنفسهم ....النخبة لتعمقهم في أسرار التقنية ولغاتها المتميزة وبرمجتها بالإضافة إلى أنهم يصفون جهات العدالة الجنائية بالقاصرين "damers "[1] وهذه مفردات الحروب الالكترونية.

ويمثل أيضا دليل آخر أمام أجهزة العدالة آلا وهو

وتحد آخر فتمثل في أن خصوصية الجريمة لها علاقة بدرجة خطورتها بالإضافة إلى وجوب أن تكون الإجراءات المتخذة_ في تتبع هذه الجرائم أو التحقيق فيها _ تتم بذات خصوصية السلوك الجرمي من حيث سرعة الحركة لتلمس الدليل وضبطه قبل نحوه أو من ناحية كيفية الضبط حيث هذه الإجراءات أن لم تكتب بسرعة وتقنية السلوك الجرمي فلا فاعلية لها ولن توصل أجهزة العدالة إلى تحقيق هدف[2].كما هو على سبيل المثال فقدان المتاجر الافتراضية بعد الحصول على منافع ربحية من معاملات وهمية، وكذلك جرائم السرقة في البنوك التجارية ومدى سرعة التحويلات النقدية ذات القيمة الفاحشة واختفاء احد عناصر العلاقة التعاقدية التجارية ويضيف البعض أن ما يرهق ويزيد من صعوبات عمل سلطات الضبط وجهاز العدالة الجنائية عموما أثناء عملية التحقيق والمتابعة مايلي:[3]

– توفر أداة الجريمة لكافة المستويات الاجتماعية والاقتصادية مع قوة عامل الإنتاج الكمي والنوعي وسرعته إلى حد وصفه بالطفرة.

– غياب التأطير النوعي لتصدي لهذا النوع من الجرائم.

– ضعف الأطر التشريعية الضابطة لهذه المعاملات وفقدان ما تعلق منها بالجانب الإجرائي والجزائي و التجريمي للمخالفات والاعتداءات الواقعة على المراكز القانونية التي تنشئها هذه المعاملات التجارية ذات الطابع الحديث في الشكل والمضمون.

– انعدام جهة قضائية جزائية مختصة في هذا النوع من الجرائم.

– وجود عروض تقدمها مواقع تجارية تسهل إجراء تعاملات التجارية وعقدها دون بيان كامل للمعلومات عن أطراف العلاقة بغرض الحصول على أرباح وجني الثروة أو على الأقل عدم تعاونها الكامل مع سلطات الضبط والاستدلال والتحقيق.

---

[1] - عبد الفتاح بيومي حجازي ، الدليل الجنائي في جرائم التزوير والإنترنت ، مرجع سابق ، ص 83 – 84، عبد الفتاح بيومي حجازي ، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت ، مرجع سابق ، ص 124.

[2] **BERTRAND WARUSFEL, Aspects juridiques de la dématérialisation des échanges dans le commerce électronique, Revue petites affiches, Droit de l'informatique, 06 février 2004 n° 27, P. 17**

[3] - عبد الفتاح بيومي حجازي ، الدليل الجنائي في جرائم التزوير والإنترنت ، مرجع سابق ، ص 84-87، عبد الفتاح بيومي حجازي ، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت ، مرجع سابق ، ص 125-129.

– جرائم التجارة الالكترونية نوع من الجرائم المعلوماتي ة والأخيرة بدورها احد الاهتمامات أجهزة العدالة الجنائية بالإضافة إلى منظومة من الجرائم التي تتصدى لها هذه الأجهزة الأمنية فيمكن بذلك إدراك حجم أو مدى أو قدرة المكافحة.

– لا تزال الخبرة الإجرائية في الضبط والتحقيق والاستدلال لدى أجهزة العدالة الجزائية بشان جرائم التجارة الالكترونية جد محدودة حيث هي(جرائم) لم تقع التنمية التي اكتسبتها أجهزة العدالة فيما يخص تعاملها مع الجرائم التقليدية، فالخبرة العملية لدى سلطات الضبط والتحقيق الجنائي تأتي من ممارسة أعمال الضبط والتحقيق ومن تم التعود والتمكن في مجال الاستدلال والتحقيق فيها.

وكمحاولة السبق هذه السلوكيات الجرمية أو على الأقل محاولة الحد من هذه الظاهرة المستحدثة لجأت بعض الدول إلى الاستيعاب، طال الأمن والقضاء ضمن المتخصصين في مجال الحاسب الآلي والمعالجة الآلية وتطبيقات المعلوماتية وقبول خبراء المعلوماتية ضمن مجال الضبط والقضاء.

ورأى البعض انه يتعين منح صفة الضبطية القضائية للمتخصصين في مجال في مجال المعلومات الأمنية إن كانو ا من أسلاك الأمن وأعوان أجهزة العدالة أو فنيين أو خبراء المعلوماتية حتى يتمكن أجهزة العدالة الجزائية من الإحاطة بمثل هذه الجرائم.[1]

وقد سلكت بعض التشريعات هذا المسلك كالمشرع الإماراتي في المادة 34 من قانون الإجراءات الجزائية إذ يحق لوزير الاتفاق مع الوزير المختص بعض الموظفين صفة الضبطية القضائية فيما يعلق من جرائم ويدخل في دائرة اختصاصهم ويتعلق بأعمال وظائفهم [2] كما أن فريق من الفقه الجنائي يميل إلى

[1] - عبد الفتاح بيومي حجازي ، الدليل الجنائي في جرائم التزوير والإنترنت ، مرجع سابق ، ص 82، عبد الفتاح بيومي حجازي ، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت ، مرجع سابق ، ص 123.

[2] - عبد الفتاح بيومي حجازي ، الدليل الجنائي في جرائم التزوير والإنترنت ، مرجع سابق ، ص 82،عبد الفتاح بيومي حجازي ، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت ، مرجع سابق ، ص 123.

المطلب الثاني : أبعاد سلطة مأمور الضبط القضائي في جمع الاستدلالات في مجال التعاملات الالكترونية

صعوبـــة الكشـــف عـــن الجرائـــم المعلوماتيـــة:[1]

جـــواز التحريـــات التـــي لا تتعلـــق بحريـــة الحيـــاة الشخصيـــة:

إذا انتهينا إلى كون رجال الضبطية يصلون إلى تفتيش الحاسب بإذن تفتيش المحل الموجود به الجهاز أو بإذن خاص فقط بالجهاز وحده عند عدم اعتبار الجهاز من مكونات المكان محل التفتيش.

فإن هذا الخلاف منشأه الحفاظ و عدم التعدي على تلك الحقوق الدستورية و أهمها الحق في الخصوصية فالجهاز بكياناته محل أوسع من المحل المادي لطبيعته المتميزة في قوة الحفظ و المعالجة، و بالمقابل نظرا لخطورة الفعل الجرمي المرتكب فإنه قد يكون من الممكن لرجال الضبط القضائي أن يقوموا بتحريات ترد على بيانات تتعلق بالمشتبه بهم طالما أن تلك البيانات لا تتضمن اعتداء على حرمة الحياة الخاصة و إن كان من الصعب السيطرة أو احترام الحدود الفاصلة بين الحق في الخصوصية و بين تتبع دليل الفعل الجرمي.[2]

---

[1] - شيماء عبد الغني ، مرجع سابق ، ص عبد الغني، ص 193.

[2] - شيماء عبد الغني ، مرجع سابق ، ص عبد الغني، ص 193،انظر أيضا :

Agathe LEPAGE, Réflexions de droit pénal sur la loi du 6 août 2004 relative à la protection des personnes à l'égard des traitements de données à caractère personnel, Revue **Droit pénal n° 3, Mars 2005, Etude 5**

حيث كل ما انتمى إلى الحياة الخاصة يقبل أن يكون محلا لجمع الاستدلالات. كما تورد التشريعات الجنائية صورا مختلفة لتجريم الاعتداء على حرمة الحياة الخاصة، و يجرم السلوك الذي يشكل فعل الاعتداء (تصوير، تسجيل محادثة).

الســـر البنكـــي:

كأصل فإن السر البنكي قد ينتمي إلى الأسرار التجارية و ليس إلى مجال الحياة الخاصة [1] ذلك أن البيانات التي يخزنها البنك هي متعلقة بسرية الحسابات المصرفية و هو محمي بنصوص معينة كالتشريع الفرنسي مثلا فهو يلزم رجل البنك بالسرية و عاقب على إنشاء معلومات سرية كل من لم يلتزم بسبب مهنته أو بسبب وظيفته أو بمقتضى مهمة مؤقتة بالحفاظ على سريتها بنص المادة 13/226.[2]

لكن مع ذلك قيد المشرع الفرنسي في قانون العقوبات عموم النص السابق بنص المادة 22/132 حين سمح بإلزام رجل البنك بتقديم ما لديه من معلومات بنكية تتعلق بالمتهم في جريمة ما و ذلك بناءا على أمر من النيابة العامة أو قاضي التحقيق أو المحكمة و نفس المنحنى تجاه المشرع الأمريكي حين استثنى من الخطر [3] الذي أقره على السلطات العامة في مسألة الحصول على ملفات العملاء من المصارف و المؤسسات المالية إلا بمقتضى أمر قضائي أو إذن تفتيش.[4]

و ذهب المشرع الفرنسي إلى أبعد من ذلك حين سمح القرار بقانون رقم 538– 2001 الصادر في 5 يوليو 2001 لوزير الداخلية في فرنسا أن يتبنى تطبيق نظام المعلومات المعالجة آليا بهدف البحث الجنائي أن تعلق الأمر بمشتبه بهم أو مجني عليهم، و هو ما يفيد جواز المعالجة الآلية في كل مراحل الإجراءات دون اعتبار ذلك مساسا بحق الخصوصية عند إطلاع رجال الضبط القضائي عليها.[5]

حق رجال الضبط القضائي في الاستعانة ببرامج الاختراق لكشف المتداخلين:

بحكم أن الجريمة قرين التطور وجب على رجال الضبط القضائي تطوير أسلوب المتابعة و الاستدلال فقد يضطر رجل الضبطية أثناء اقتفاءه لأثر المقتحمين أو المجرمين إلى استعمال مصادر تزوده بالمعلومات و استخدام برامج معدة سلفا أو الاستعانة بمرشد سري، على شرط عدم التعدي على حق الخصوصية و احترامه، إلا عند الاقتضاء كما سنرى.

الكشف عن هوية المشترك و حركة اتصالاته من جانب مزود الخدمات:

---

[1] - قضى في و م أ (حكم Miller) بأن الشرطة لها أن تأمر البنك بتقديم معلومات عن شيك خاص يأخذ عملاتها.

[2] - المادة 13/226 عقوبات فرنسي النص، حرفيا عند شيماء عبد الغني ، مرجع سابق ، ص عبد الغني، ص 197، الهامش (1).

[3] - شيماء عبد الغني ، مرجع سابق ، ص عبد الغني، ص 197.

[4] - 12 USC §§ 3401 -3422 ، شيماء عبد الغني ، مرجع سابق ، ص عبد الغني، ص 197.

[5] - شيماء عبد الغني ، مرجع سابق ، ص عبد الغني، ص 198.

من واجب مزود الخدمات التعاون مع رجال الضبط القضائي بتزويدهم ببيانات تتعلق بهوية المشترك و الأرقام التي اتصل بها الكترونيا دون إعطاءه بيانات تتعلق بمحتوى و مضمون الاتصال ذاته حيث لا تتعلق الأولى بحرمة الحياة الخاصة و هو ما أجازته الاتفاقية الأوروبية المتعلقة بجرائم السيبر له 2001.[1]

حين سمحت في المادة 18 منها لسلطاتها بالتحري عن البيانات المتعلقة بالمشترك و لو تعلق الاتصال بأكثر من مزود للخدمات و تعرض لبيان المقصود من تلك البيانات بكونها " تتعلق بنوع خدمة الاتصال التي اشترك فيها الشخص و الوسائل الفنية..... و مدة الخدمة و شخصية المشترك و رقم دخوله للحصول على تلك الخدمة و الفواتير التي ترسل إليه و أي معلومات تتعلق بطريقة الدفع أو أي معلومات أخرى تتعلق بأداء الخدمة أو بالاتفاق بين هذا المشترك و مزود الخدمة". [2] و الذين لهم حق الاطلاع على هذه المعلومات في إطار التحقيق الجنائي (م 151 من قانون الإجراءات الفرنسي) هم أعضاء النيابة العامة و قضاة التحقيق و الحكم و مأموري الضبط القضائي المختصين [3] حماية للحرية الشخصية و حصر الإطلاع على هذه المعلومات على أشخاص معينين هو شرط أساسي لقبول الأدلة التي تم الحصول عليها بطريق مباشر أو غير مباشر من هذه الملفات.[4]

و لعل هذه الاتفاقية قد عززت من قاعدة التعاون الإقليمي بين أعضاءها في منطوق المادة 18 حيث أعطت للدولة الطرف الحق في آن تشرع ما يتيح لسلطاتها المختصة الحق في أنه تأمر أي شخص متواجد على إقليمها يحوز تلك المعلومات مخزنة في أي وسيلة تخزين متعلقة بالكمبيوتر أو مزود الخدمات يقدم خدماته في إقليم الدولة أن يقدم المعلومات التي لديه المتعلقة بالمشترك في تلك الخدمات في حيازته أو تحت سيطرته.[5]

و هذا التوسع يظهر أكثر لدى الدول الأنجلو سكسونية [6] حيث يعطي القانون الانجليزي – الصادر عام 1984 بشأن البوليس و الأدلة الجنائية – للمحققين أن يطلبوا من الغير (دون

---

[1] **Nathalie DREYFUS, De la responsabilité des intermédiaires techniques : contrefaçon ou responsabilité civile ? Revue Communication Commerce électronique n° 1, Janvier 2007, Alerte 1**

[2] - شيماء عبد الغني ، مرجع سابق ، ص عبد الغني، ص 205.
[3] - حسل عبد الباقي الصغير، أدلة الإثبات الجنائي، ص 101.
[4] - جميل عبد الباقي الصغير ، مرجع سابق ، ص، أدلة الإثبات، ص 102.
[5] - شيماء عبد الغني ، مرجع سابق ، ص عبد الغني، ص 206.
[6] - أفرد التشريع الأمريكي قانونا خاصا متضمنة مواده تعاون متعهدي خدمات الرسائل في مجال الاتصالات الالكترونية المسجلة مع الأجهزة القضائية، جميل عبد الباقي الصغير ، مرجع سابق ، ص، أدلة الإثبات، ص 107.

تحديد صفة أو هوية هذا الغير) أن يمكنوهم من الدخول إلى المعلومات المخزنة في الحاسب الآلي أو الإطلاع عليها أو قراءتها.[1]

كما يجيز القانون الأمريكي جواز تفتيش الكمبيوتر في حالة الضرورة الإجرائية.[2]

المطلب الثالث : مبادرات المشرع المقارن لتقنين الإجراءات الجنائية للعالم الرقمي:[3]

سعيا من كثير من المشرعين للإحاطة في تأطير القاعدة الإجرائية بالشرعية و نستعرض موقف المشرع الأوروبي و الأمريكي:

الفرع الاول : المشـــــرع الأوروبي:

للمجلس الأوربي دور هام في مواجهة جرائم المعلوماتية من خلال إقراره للعديد من التوصيات، و إصداره لقواعد توجيهية في هذا المجال تضمنت وجوب الدعوة إلى تجريم العديد من الأفعال..... إلى جرائم هذا النوع كالغش المعلوماتي، التزوير الالكتروني، سرقة منفعة الحاسب الآلي، الدخول غير المصرح به إلى نظم المعالجة الآلية للبيانات مثلما أن هذه المجهودات تعلقت أيضا بالنص على قواعد خاصة بالجوانب الفنية.4

و لعل أهم نشاطات المجلس هو إصداره لاتفاقية شاملة متعلقة – بجرائم الحاسب الآلي Droft Conrention on Cyber Crime – starsbourg le 25/04/2000 حيث نبهت فيها إلى خطورة هذه الجرائم و مدى الجهد الذي يستلزم بذله في إطار البحث عن الأدلة و الإثبات هذا للطبيعة الخاصة التي تتمتع بها هذه الجرائم[5].

كما أكدت الاتفاقية على التوصيات NR (89)9 المتعلقة بالمشاكل التي تعيق قانون الإجراءات الجنائية في مجال جرائم الحاسب الآلي6 هذه التوصية التي أصدرها المجلس الوزاري الأوربي في أصدرها المجلس الوزاري الأوروبي في 1995/09/11 توصية رقم 95/13 متعلقة بمشكلات الإجراءات الجنائية المتعلقة بتكنولوجيا المعلومات بعد لاحظ أهمية و

---

[1] - جميل عبد الباقي الصغير ، مرجع سابق ، ص، أدلة الإثبات، ص 106- 107.

[2] - شيماء عبد الغني ، مرجع سابق ، ص عبد الغني، ص 207.

[3] - عمر محمد أبوبكر بن يونس ، مرجع سابق ، ص788.

[4]- عبابنة الرزاقي، ص 164 / محمد مسعود محمد خليفة، الحماية لمعطيات الحاسب الآلي، ماجستير، الاسكندرية، ص 206، ص 72.

[5] Antoine LATREILLE, LA PROTECTION JURIDIQUE DES BASES DE DONNEES ELECTRONIQUES, Revue petites affiches, Droit de la communication, 28 avril 1995 n° 51, P. 14

[6]- عبابنة الرازقي، ص 165.

ضرورة تقنية القاعدة الإجرائية و ميزت بين التفتيش و الضبط و نص في بعض موادها على:[1]

المادة 01 التمييز بين التفتيش و الضبط

المادة 05 المراقبة التقنية

المادة 09 إلزامية التعاون مع جهات التحقيق و الدليل الإلكتروني

المادة 14 استعمال التشفير

المادة 15 أهمية تدريب و تطوير البحث العلمي

المادة 17 التعاون الدولي و ضرورته.

الفرع الثاني : المشرع الأمريكي

حاول المشرع الأمريكي الحفاظ على التوازن القائم بين محاولة رصيد القاعدة الإجرائية التي تتناسب مع تكنولوجيا المعلومات و بين الحقوق الدستورية المتعلقة بحماية حق الفرد في خصوصية و فق الخصوصية وفق النصوص[2]

مستعينا في ذلك بالجهاز وفق ما يصدر عنها في المرشد الفيدرالي للإجراءات الجنائية للجرائم الناشئة عن الحواسب و تكنولوجيا المعلومات كمرشد مساعد للقائمين على التحقيق و المحاكمة على شاكلة المرشد الفدرالي لتفتيش و ضبط الحواسيب كعون للجهات القضائية في تقصي جرائم الحاسوب و الإنترنيت و أصدرت عليه ملاحق سنة 1997 و آخر في 1999، و أصدرت إدارة العدل الأمريكية النسخة المنقحة بعنوان نظم تفتيش و ضبط الحواسيب و الحصول على الأدلة في التحقيقات الجنائية[3].

و يعتبر هذا المرشد .....لسلطات الضبط القضائي في مرحلة الاستدلال و التحقيق حيث تقوم الفكرة المبنى عليها المرشد على عملية إحداث اتصال بين الضبط القضائي و عناصر التحقيق و بين الدليل الإلكتروني أو الرقمي و كيفية الحصول عليه قصد الوصول إلى المحاكمة الجنائية[4]

و تضمن هذا المرشد الصادر في 2001 خمسة أبواب[5]:

الباب الأول: موضوع التفتيش و ضبط الأدلة من الحاسوب دون إذن تفتيش.

الباب الثاني: موضوع التفتيش و ضبط الأدلة بالاستناد إلى إذن التفتيش.

الباب الثالث: موضوع التعامل مع وسائط الاتصالات المقررة في قانون الخصوصية.

---

[1] - عمر محمد أبوبكر بن يونس ، مرجع سابق ، ص788.

[2] - - عمر محمد أبوبكر بن يونس ، مرجع سابق ، ص789.

[3] - عبابنة –الرزاقي ص0148/142 عمر محمد أبوبكر بن يونس ، مرجع سابق ، ص789.

[4] - عمر محمد أبوبكر بن يونس ، مرجع سابق ، ص790.

[5] - عمر محمد أبوبكر بن يونس ، مرجع سابق ، ص790- 791.

الباب الرابع: موضوع المراقبة الالكترونية

الباب الخامس: موضوع كيفية التحفظ على سجلات الحاسوب، و سماع الشهود

و عدلت هذه النسخة سنة 2002 و أحدثت تعديلات عليه تناولت الإجراءات الجنائية عبر الانترنيت.[1]

المطلب الرابع : مراحل الدعوى الجنائية في جرائم التجارة الالكترونية:

إن التنازع حول الاختصاص القضائي في جرائم التجارة الالكترونية نرشح أنه لن يكون تنازعا بين فكرة الإقليمية و الدولية فقط بل يستمد هذا النزاع إلى داخل حدود الدولة الواحدة يعني أن قواعد الاختصاص الداخلي في الدولة سوف تكون عرضة للتغيير و محلا للدراسة و البحث من قبل الجهات التشريعية القضائية.[2]

و الفقه القانوني الجنائي اهتم بمسألة الاختصاص القضائي في مسائل الجرائم المعلوماتية كإشكالية (واجبة الحل) قائمة متمثلة في صراع بين مدى كفاية التقاضي التقليدي ليكون كفيلا بالنظر بالدعوى الجنائية في قضايا التجارة الالكترونية و بين إمكانية قيام قضاء مختص في مثل هذه الجرائم على غرار القضاء المختص في فروع القانون المختلفة.[3]

حيث إن الجرائم المرتكبة في إطار التجارة الالكترونية لا تتحدد بمكان معين كما ينطبق هذا الوصف على النتيجة الإجرامية و هو ما يطرح إشكالية تنازع القوانين فالتفسير المبني على أساس النظرية التقليدية القاضي باختصاص الدولة التي ارتكب فيها النشاط الإجرامي. كما تلك تحققت فيها النتيجة الإجرامية و هو ما يطرح إشكالية قد يكون مفيدا التفسير مرحليا إلى حين تكون رؤية قضايا واضحة المعالم لمدلول العلم الافتراضي، فجرائم التجارة الالكترونية الواقع في العالم الافتراضي يجعلها ذات انتشار يتجاوز الحدود السياسية و الجغرافية يجعل الاختصاص القضائي منعقدا لكافة المنظمة القضائية في العالم المادي [4] و هذا ما يدعوا إلى طرح تساؤل هو كيفية نفاذ التشريع في الواقع المادي لحماية العالم الافتراضي و تحديد المسؤولية الجنائية لمن اعتدى على مراكز يحميها القانون خاصة أن البنية التحتية للتجارة الالكترونية تفتقد الآلية التي يمكن بواسطتها تحديد شخصية الجناة[5].

الفرع الأول : مرحـــلة جمـــع الاستـــدلالات:

---

[1] - عمر محمد أبوبكر بن يونس ، مرجع سابق ، ص791.

[2] - عمر محمد أبوبكر بن يونس ، مرجع سابق ، ص795.

[3] - عمر محمد أبوبكر بن يونس ، مرجع سابق ، ص795.

[4] - عمر محمد أبوبكر بن يونس ، مرجع سابق ، ص795.

[5] - حيث غاية ما تستطيع أن تكشفه آلياتها هو تحديد وسيلة ارتكاب الجريمة أو تحديد الحاسوب الذي انطلق منه السلوك الإجرامي في ثوبه التقني، للإطلاع محاولة الإجابة على هذا التساؤل أنظر عمر محمد أبوبكر بن يونس ، مرجع سابق ، ص796- 807

مرحلة جمع الاستدلالات من أهم مراحل بناء الدعوى الجنائية حيث ينظر لها التشريع و الفقه بإمعان مؤكدا على الدور الرئيسي الذي يقوم به الضبطية القضائية لكونه يعد خط الدفاع الأول ضد الجريمة.[1]

الضبـــط الإداري و الضبـــط القضائي[2]

01- سلطات أجهـــزة الضبـــط القضائي

.....

أ/ المجـــال الإقليمـــــي:

انعقد مؤتمر في أوسلو (النرويج) بتاريخ 29-31 ماي 2000 ضمن القائمين على سلطات الضبط القضائي في القانون المقارن أهم موضوع نوقش فيه هو عدم إمكانية البنية التحتية للمعلوماتية من التوصل إلى تحديد شخصية مرتكب الجريمة أو المصدر الحقيقي لها، و موقعه على وجه التحديد و أما السلطات تحتاج إلى صلاحيات أكثر لكي يتم ضبطه الشخص مرتكب الجريمة لأنه من غير الممكن القيام بتحديد هوية مرتكب جريمة ليس لها حدود الكترونية بالأخص إذا كان الجاني محترفا في برمجيات التخفي.[3]

و قد اجتهد المشرع الأمريكي و الألماني و البريطاني و الصيني في إعداد قوات خاصة لمواجهة الجرائم الالكترونية *Anti- hacking tosk forces* معتمدة في تكوينها تكوينا علميا تكنولوجيا لأفرادها، و كلفت هذه القوات هي نظم الإنترنيت أي تتبع و مطاردة كل مجرمي المعلوماتية المحترفين و قراصنته ا[4]، و قد أحست هذه الدول و غيرها بخطورة الجرائم الالكترونية المنعقد في أكتوبر 2000 و من نتائج هذا المؤتمر الدعوى إلى ضرورة التعاون بين التجار و الحكومات لأجل التقليل من خسائر الجريمة في العالم الافتراضي.[5]

أما المشرع الفرنسي فيملك آلية التعامل مع هذه النوعية من الجرائم بكفاءة كبيرة بواسطة جهاز متخصص هو مؤسسة حماية البرمجية *Agence pour la protection des programmes*.

ب/ المجـــال الدولـــي:

ما عدا المباحث الفدرالية الأمريكية فإن الضبط القضائي حول العالم لم تترك إلا في نطاقها الإقليمي،و يمكن رصد دور تقوم به منظمة التعاون الإقتصادي و التنمية لمعالجة لإشكاليات مواجهة الإجرام المعلوماتي، كما قامت مجموعة الثمانية الاقتصادية و منظمات دولية أخرى و

---

[1] - عمر محمد أبوبكر بن يونس ، مرجع سابق ، ص807.

[2] - عمر محمد أبوبكر بن يونس ، مرجع سابق ، ص808- 810.

[3] - عمر محمد أبوبكر بن يونس ، مرجع سابق ، ص810- 811.

[4] **Bruno P. LANGLOIS, La protection des marques sur internet : le législateur fédéral américain s'attaque à la cyberpiraterie, Revue Gazette du Palais, 20 juillet 2000 n° 202, P. 29**

[5] - عمر محمد أبوبكر بن يونس ، مرجع سابق ، ص813.

بعض الدول بإعداد ملتقى دولي في نهاية عام 2000 بطوكيو لتكوين قوة دولية أطلق عليها *digitale opportunity tosk force* مهمتها تحقيق أمن تكنولوجيا المعلومات[1].

و لعل بعض صور هذا التعاون هو السابقة التي تعقبت فيه المباحث الفدرالية و الشخص الذي زرع فيروسا عبر الانترنيت أحدث الأخير للسلطات الفيليبينية.[2]

و كذلك تعاون المباحث الفدرالية الأمريكية مع البوليس الانجليزي و كان نتيجة هـــذا التعاون هو كشف عن أول حادث اختراق في مقاطعة ويلز سنة 2000[3]

02- النطاق الإقليمي في اختصاص الضبط القضائي:[4]

مسألة الاختصاص القضائي لأمور الضبط القضائي من المسائل المعقدة في إطار المسار الذي ينساق إليه القانون عقب هذه الثورة، و حيث يتطلب القانون الالتزام بالنطاق الإقليمي فإنه في سابقة قضائية ما ذهبت إليه محكمة النقض الفرنسية في حكم صدر لها في 10-01-1992 متعلق بتطبيق المادة 1/18 (من قانون إ ج فرنسي) حيث استخدمت في منطوق حكمها تمييزا بين تصرفين الأول هو:[5]

أن يقع خروجه عن نطاق اختصاصه الإقليمي تحت طائلة النقض و الإبطال حين يكون خروجه ماديا و هذا الفعل هو متعارض مع نص المادة المذكورة، قيام مأمور الضبط القضائي باستطلاع ملفات "عن بعد" بقصد القيام بتحريات لازمة حول وقائع تعرض عليه، و اعتبر الحكم أن ما يحصل عليه مأمور الضبط القضائي من وصول بلاغات أو وثائق و مستندات... من خارج نطاقه الإقليمي لم يكن بتحصيله متجاوزا لنطاقه الإقليمي، فهو لم ينتقل ماديا إنما وصلت الوثائق إليه من خارج دائرة اختصاصه بوسائل تقنية الكترونية إنما هي معلومات مشروعة فهو لم يتجاوز نطاق اختصاصه الإقليمي في تحصيلها بل جاءت إليه، يعني ذلك إمكانية امتداد النطاق الإقليمي لمأمور الضبط القضائي خارج نطاق الحدود المقررة قانونا دون أن يخشى تعرض ما يحصل عليه من تحريات عن طريق المعلوماتية للإبطال لكون هذا التجاوز لم يكن ماديا و إنما يظل في النطاق المعنوي المعلوماتي[6].

---

[1] **Bruno P. LANGLOIS, La protection des marques sur internet : le législateur fédéral américain s'attaque à la cyberpiraterie, Revue Gazette du Palais, 20 juillet 2000 n° 202, P. 29**

[2] - لم تكن الفيليبين تدرك وجود قدرات تكنولوجية عند أفراد شعبها مما دفع البعض إلى التأكيد على أن شرع الدول التي تنخرط في المنظومة الرقمية إلى سن تشريعات تتصدى لمفردات الإجرام المعلوماتي كما أوصى مدير تحقيقات الحاسوب في مركز حماية البنية التحتية التابع للمباحث الفدرالية الأمريكية حين صرح بأن هناك العديد من الدول التي تسعى لكي تكون جزءا من الاقتصاد العالمي و التجارة الالكترونية و هي تمهد لشعوبها كذلك، و ليست لديها قوانين تتعامل مع هذه الظاهرة. 815.

[3] - عمر محمد أبوبكر بن يونس ، مرجع سابق ، ص814- 815.

[4] - عمر محمد أبوبكر بن يونس ، مرجع سابق ، ص815- 816.

[5] - عمر محمد أبوبكر بن يونس ، مرجع سابق ، ص815- 816.

[6] - عمر محمد أبوبكر بن يونس ، مرجع سابق ، ص816.

إذا كانت مبادئ الضبط القضائي هي تلك الصلاحيات التي يمنح (المأمور به) لرجاله ليباشروا مهامهم في إطار رصد جرائم التجارة الالكترونية فإنه في هذا الإطار يتفق الفقه و القضاء على أن أعمال الضبط القضائي لا تقع تحت حصر لذلك منحهم القانون سلطة الاستعانة بالجزاء أثناء جمع الاستدلالات بشرط _ كما يرى الفقه _ أن يكون هناك جريمة وقعت حيث الخبرة في مرحلة جمع الاستدلالات تعد أيضا حالات علمية تقنية لها مدلولها التوضيحي، كما لها أثرها القانوني إذا أثبتت في محضر جمع الاستدلالات المعد من قبل مأمور الضبط و يخضع المحضر للسلطة التقديرية الكاملة لقاضي الموضوع.[1]

03- مبـــدأ التخصـــص في عمـــل مأمـــور الضبـــط:

نقصد بالتخصص مدى..... عمل الضبط القضائي و موضوعاته لكي يكون مأمور الضبط القضائي (على استعداد) و ذو كفاءة للتعامل مع هذا النوع من الجرائم و نقصد كذلك بالتخصص موضوع تقدير قيام الجريمة و لزوم تدخل مأمور الضبط و توقيت ذلك.[2]

و مسألة التخصص تطرح من جوانب عدة منها:

صعوبة الكشف عن الجرائم المعلوماتية و معرفة مرتكبيها

عدم التبليغ من طرف قبل المؤسسات و المجني عليهم خوفا من فقد ثقة العملاء و المساس بالسمعة التجارية.[3]

و تطرح مسألة التخصص عدة مسائل ذات الحساسية في مجال عمل مأمور الضبط القضائي إذ يتساءل البعض هل يقصد بالتخصص هو رصد أجهزة خاصة للتعامل مع هذا الصنف من الجرائم حتى يقترب عمل مأمور الضبط أو يكون عمل خبير.[4]

و يرجح أن يعتمد إلى إيجاد تخصصات لمجموعات من مأموري الضبط في إطار أنظمتهم، يجعل من متابعة هذه الجرائم و ضبطها يقوم بشكل آلي مباشر.[5]

أ/ مصطلحـــات التخصـــص:

أفرز التعامل الإنساني مع شبكة المعلوماتية في الفترة الأخيرة إلى استحداث مصطلحات لمتعاملين متقابلين أحدهما إيجابي و آخر سلبي.

---

[1] - عمر محمد أبوبكر بن يونس ، مرجع سابق ، ص817.

[2] - عمر محمد أبوبكر بن يونس ، مرجع سابق ، ص818.

[3] - شيماء عبد الغني ، مرجع سابق ، ص عبد الغني 197.

[4] - هذا ما جعل البعض يدعوا إلى التخلي عن رصيد ميزانيات إعداد الأجهزة و العناصر المخصصة في التعامل مع جرائم التجارة الالكترونية و بصفة عامة تكنولوجيا المعلومات في مقابل منح صفة الضبط القضائي لمجموعة خبراء المعلوماتية الذين وصلوا درجة الاحتراف. 819.

[5] - عمر محمد أبوبكر بن يونس ، مرجع سابق ، ص820.

فالإيجابي: من أبرز تجلياته معاملات التجارة الالكترونية بالإضافة، التوظيف العلمي لها حركة البريد الالكتروني... و هذه المصطلحات متخصصة من حيث اللغة و البرمجة و التجاوب ، كما أن هذا الجانب خلق نقيضه أي ذلك التفاعل الإنساني السلبي وصل إلى ارتكاب عبر ذات الوسيلة التي حققت منافع جمة و بدورها لها مصطلحات جرمية خاصة بها هذا الأمر امتد ليشمل مؤسسات مكافحة الجريمة لكي يكون لها مصطلحاتها و تطوير تلك المؤسسات يمكنها مواجهة نمط الجريمة المستحدث، نشير إلى أن وقوع جرائم تمس بالتجارة الالكترونية يستدعي كما يرى البعض إعادة النظر في تفسير المشروعية في بعض أعمال الضبط القضائي كما هو الشأن في التخفي عبر الاتصالات، و انتحال اسم وهمي دخول حلقات النقاش.. تقصد الكشف عن الجرائم.[1]

04- لـــزوم تدويـــن الإجراءات الجنائيـــة:

05- الحصـــول عـــلى الإذن القضائـــي:

قلصت المعلوماتية المنطق القضائي التقليدي في مسألة الحصول على إذن لرجال الضبط القضائي لمنحهم صلاحيات التدخل لممارسة أعمال الضبط، حيث الحصول على إذن التفتيش و الضبط و حتى القبض حصل لها تحول جذري بتغير نمط المعاملات التجارية و تغير معطيات المعاملات فانعكست أيضا على أسلوب ضبط هذه الجرائم الواقع على هذه المعاملات فأصبح ذلك ممكنا من خلال اعتمادات التقنية التي تتسم بها المعاملة و الكيفية التي ترتكب بها الجريمة، كما لو كان مثلا مأمور الضبط في أحد حلقات النقاش و انتهى إلى علمه وقوع جريمة أو ينخرط في حلقة نقاش تقضي إلى الدعاية أو عرض مواقع إباحية بالجنس أو المخدرات أو غير ذلك من المجالات غير المشروعة مما يجعله يتولى مباشرة مهامه بالصورة التي تحقق الهدف من أعمال الضبط و عدم تجاوزه لصلاحياته.[2]

كأصل عام ليس لرجل الضبط القضائي أن يتجاوز صلاحية الضبط القضائي خارج نطاق تخصصه في نطاق الإجرام العادي. إلا أنه و لأجل مواجهة جرائم مثل جرائم التجارة الالكترونية فإن الأمر يحتاج إلى إعادة تفسير حيث تتجاوز هذه الجرائم كل الحدود، و هذا ما جعل من الممكن تقرير نص بمقتضاه السماح لرجال الضبطية القضائية الانتقال عبر شبكة المعلوماتية للتعاون مع جهات ضبط دولية بالأخص أنه لا يوجد ما يمنع ذلك و ليس له مساس نطاق التخصص الإقليمي، حيث هذا الانتقال ليس ماديا لرجال الضبط بل الانتقال لواقع هو التعاون أمني وفق ما تقرره اتفاقيات دولية لمكافحة الإجرام المعلوماتي أو انتقال رقمي يكون

---

[1] - عمر محمد أبوبكر بن يونس ، مرجع سابق ، ص822.

[2] - عمر محمد أبوبكر بن يونس ، مرجع سابق ، ص823.

التعاون فيه مع جهات أخرى خارج نطاق اختصاصه المكاني في الوقت الذي يكون فيه ماديا موجودا في نطاق اختصاصه المكاني.[1]

هذا الطرح يتطلب تقريره نص خاص لخطورة الموقف الذي تعالجه في إطار عمل الضبطية القضائية لما يمكن أن يترتب عليها قبولا من قبل القضاء أو رفضها لما يرتب بطلان الإجراءات، صدر قانون سمي بـــ *Patriot Act* بالولايات المتحدة الأمريكية عقبت أحداث ديسمبر 2001 منحت بمقتضاها سلطات مخابرات أمريكية كالمخابرات الأمريكية *CIA* و هيئة الأمن القومي *NSA*، و الخدمات السرية *SS* و الاستخبارات العسكرية، صلاحية الإطلاع على التحقيقات التي تمارسها جهات الاستدلال و التحقيق *FBI* دون بيان حدود الكيفية التي تستخدمها جهات الضبطية و دون الرجوع إلى الجهات القضائية للحصول على إذن بذلك.[2]

أ/ البـــــلاغ:

تلقى التشريعات المقارنة التزاما على عاتق رجال الضبط القضائي حين تلقيهم معلومات حول واقعة ما موصوفة بأنها جريمة في القانون بتدوينها في محاضر و الاستيضاح بشأنها (المادة 24 إ ج مصري).

و البلاغ هو أخطر أدوار تعامل السلطات مع الظاهرة الإجرامية كونه يعد وسيلة التعبير المباشرة عند مدى تملك جهات الاختصاص بتنفيذ القانون.[3]

و دور المجني عليه دور جدي في صد مثل هذا النوع من الجرائم، ولعل هذا الدور هو الوحيد في الكشف عن هذه الجرائم دون أن يكون لذلك ارتباط بقيود للدعوى الجنائية كالشكوى و الإذن و الطلب، و هذا دور بأنه من الأهمية التي لا يمكن الاستهانة به لكون مثل هذه الجرائم ذات جديد و ليس لها سوابق و إن كان في عملية الإبلاغ بعض الضرر على المجني عليه.[4]

و لأجل تسهيل هذه الخطوة فقد مكنت بعض التشريعات الأفراد المستهلكين و المجني عليهم من تسجيل بلاغاتهم و التحقق فيها و الحصول على الاستيضاحات بشأنها و إجراء المعاينات الالكترونية، و قد نشطت عملية الضبط القضائي الالكتروني بواسطة مواقع أنشأت خاصة بالبلاغات المتعلقة بهذه الجرائم و إرساله إلى جهات مختصة[5] و لها مواقع تخص الضبط

---

[1] - عمر محمد أبوبكر بن يونس ، مرجع سابق ، ص823.
[2] - عمر محمد أبوبكر بن يونس ، مرجع سابق ، ص823.
[3] - عمر محمد أبوبكر بن يونس ، مرجع سابق ، ص824.
[4] - عمر محمد أبوبكر بن يونس ، مرجع سابق ، ص825.
[5] - موقع المباحث الفيدرالية الأمريكية FBI، موقع إدارة العدل الأمريكية USDOJ، موقع البلاغات للمخابرات المركزية الأمريكية CIA، موقع هيئة حماية البرمجيات الأوروبية.

القضائي المتخصص في حماية المستهلك و التبليغ عن جرائم الاتجار غير المشروع الذي يتم الكترونيا.[1]

و لعل الإشكال الذي يمكن أن يطرح هو مدى القيمة القانونية لمثل هذه التبليغات الالكترونية و الأثر القانوني للتحريات التي تجريها برمجيات الكترونية و هل تقبل الضبطية القضائية و جهات التحقيق مثل هذا النوع من التبليغات؟[2]

(للإجابة عن هذا التساؤل) إن البلاغ في ذاته هو محل بحث و تحر، لمقوماته تكتمل بعد التأكد من مصداقيته، و يسأل مأمور الضبط القضائي إن أهمل في ذلك، حيث يجب عليه تناول البلاغ بجدية كاملة و القانون يعلق مسؤولية مأمور الضبط القضائي على العلم بالبلاغ و عاقبه على كل إهمال أو تأخر في اتخاذ الإجراءات التي يتطلبها القانون بعد علمه.[3]

و يستوي أن يكون البلاغ ماديا بحضور الشخص مثلا إلى مركز الشرطة أو يكون البلاغ معنويا كأن يكون وارد من مجهول أو رقميا كالبلاغات التي ترد عن طريق الانترنيت حين يتطلب الأمر الدخول إلى أحد المواقع الخاصة بالبلاغات و ملأ البيانات الخاصة بالبلاغ و إرسالها إلى الجهات المختصة بتلقي هذه البلاغات.[4]

و منه نقول أن للبلاغ قيمة قانونية حينما يتم بهذه الطريقة ذلك أنه مؤشر على وقوع جريمة يوجب على رجال الضبطية القضائية تتبع البلاغ و إجراء التحديات اللازمة حول ما ورد فيه، لا عبرة بما يشتمل عليه البلاغ عن الجريمة حسبما يرد في محضر جمع الاستدلالات و إنما العبرة بما تقتنع به المحكمة مما تستخلصه من فهم الواقعة بمعنى مثلا أنه إذا ورد في محضر الاستدلالات أن البلا غ هو بشأن سرقة حدثت و تبين للمحكمة أن الواقعة هي اختلاس مال عام فإن ذلك لا يتأثر فيما تستقر عليه فهم محكمة الموضوع، و وصول بلاغات عن وجود مواقع أو صفحات خادمة أعدت للاحتيال على الناس دون الإفصاح عن هوية المبلغ فإن البلاغ يظل قائما حتى على افتراض أن الموقع ليس من المواقع الاحتيالية الخادمة بل نشاط الموقع مرتكز على التجارة غير المشروعة فإن عدم الدقة في تصوير الواقعة لا يؤثر على عقيدة المحكمة و على قاضي الموضوع.[5]

---

[1] - عمر محمد أبوبكر بن يونس ، مرجع سابق ، ص826.

[2] - عمر محمد أبوبكر بن يونس ، مرجع سابق ، ص826.

[3] - توجد هناك لتكملة عمل الضبطية القضائية منظمات إنترنيت مدنية تنشط في مجال التعامل مع البلاغات لتدارك أي نقص يمكن أن يحدث من طرف الجهات الإدارية و القضائية الرسمية المختصة، هذه المنظمات تتولى متابعة البلاغات التي ترد إليها و يطلعون على حيثياتها و يتصلون بالضحية و إن كان خارج حدود الدولة لمتابعة و اطلاع الضحية بآخر التطورات بموضوع البلاغ على شاكلة موقع INFOWAR الذي يكاد يتطابق مع عمل جمعيات حماية المستهلك الحديثة، عمر محمد أبوبكر بن يونس ، مرجع سابق ، ص826.

[4] - عمر محمد أبوبكر بن يونس ، مرجع سابق ، ص827.

[5] - عمر محمد أبوبكر بن يونس ، مرجع سابق ، ص828.

أمر آخر متعلق بحساسية التحريات التي تجريها برمجيات ذكية و قيمتها القانونية حيث يجب التركيز على عامل الزمن و الوقت. فيجب أن يكون للاستدلال الذي يجريه رجال الضبط القضائي بعدا أكبر في الاهتمام بجانب التحريات حتى لا تفقد الأدلة وجودها بفعل الزمن انتظارا لسلطات التحقيق في هذا الشأن.

و لا يختلف البلاغ من حيث الأهمية في الطابع التقليدي عنه في الطابع الرقمي يعني أن تلقي البلاغ في العالم الافتراضي له ذات الطبيعة في العالم المادي.

ب/ الشكـــــوى:

06- نظـــام الإرشـــاد الجنائـــي عبـــر الانترنيـــت:

قد تتسع عملية البحث عن جريمة مرتكبة إلى جواز استعانة مأموري الضبط القضائية بمرشدين دورهم إمداد مأموري الضبط القضائي بالمعلومات عن الجرائم و مرتكبيها و هذا النظام معترف به في القانون الجنائي و يمتد الأمر إلى القيام بإعداد مرشدين جنائيين و زرعهم في مهام البحث عن الجريمة و مرتكبيها.[1]

أ/ المرشـــد المعلوماتـــي الجنائـــي:

تبرز أهمية نظام الإرشاد الجنائي المعلوماتي (الالكتروني) في كونه يرسى بنيان جنائي للمعلوماتية يحاصر النشاط الجرمي.[2]

يستخدم هذا النمط من المرشدين من قبل العديد من المؤسسات الضبطية حول العالم حيث ترفع بعناصرها و تجندهم مع الغير للدخول إلى المجالات الرقمية عبر حلقات النقاش و قاعات البحث و الاتصال المباشر باستخدام أسماء وصفات مستعارة و وهمية قصد البحث عن الجرائم و مرتكبيها و تقديمهم إلى المحكمة.[3]

و يمكن لرجل الضبطية القضائية أن يقوم بدور المرشد الجنائي بعد الحصول على إذن رسمي بمباشرة مهامه عبر الانترنيت ثم استغلال حاسوب متصل بالشبكة سعيا وراء الكشف عن جرائم و مرتكبيها بالآليات التي تمنحها التقنية، الدخول إلى قاعات دردشة أو حلقات نقاش أو استخدام برمجيات إلى اللحظة التي يبرز فيها مشروع إجرامي من قبل الغير (اتجار غير مشروع، تحويل سرقة اختلاس أموال..... وهمية، اختراق شبكات و مواقع تجارية، اختراق شبكات و مواقع تجارية، الترويج لبرمجيات مسروقة و محاولة تسويقها) فيكون للمرشد الجنائي القيام بمقتضى المعلومات المتعلقة بالفعل الجرمي و بيان معلومات متعلقة بالجاني.

---

[1] - عمر محمد أبوبكر بن يونس ، مرجع سابق ، ص837.
[2] - عمر محمد أبوبكر بن يونس ، مرجع سابق ، ص839.
[3] - عمر محمد أبوبكر بن يونس ، مرجع سابق ، ص838.

ثم يقوم المرشد الجنائي بتوصيل هذه المعلومات إلى جهة الضبط القضائي التي تباشر تحرياتها في ضبط الجريمة باستخدام برمجيات معينة تقودها إلى مزود الخدمات الذي يتحرك فيه مرتكب الجريمة أو تقوم باستدراجه حال التعرف لنواياه [1]، و تستخدم كذلك آلية المراقبة البرمجية و إن كانت هذه الآلية محل نظر قانوني من حيث ضرورة التقييد.

حيث ضرورة التقييد بها و اعتمادها كأسلوب بحث و تحري و بين ضرورة الالتزام بما هو مقرر قانونا كحقوق مشكلة في ضمانات دستورية حيث البرمجيات التي تعتمد في البحث عن الجرائم و مرتكبيها كبرمجية *Carnivol* و ملفات *SQL* من مايكروسوفت و هي برمجيات هي مرحلة تطوير و هي برمجيات قد لا تتوافق مع الضمانات الدستورية الفردية.[2]

07- تقييـــد الحريـــة:

كأصل عام لا تمتد الصلاحيات الممنوحة لرجال الضبط القضائي إلى تقييد حرية الأشخاص أو التعدي على حقهم في الخصوصية لكن قد لا يكون لهذه القاعدة استثناء إذا ما تمت استثناء إذا ما ثبت اتهام شخص بسلوك موصوف قانونا بأنه جريمة حيث يبيح القانون المأمور الضبط إجراءات تقييد من حرية هذا الشخص و هذا إجراء لا يطرح إشكال إذا كان موضوع هذه الجرائم تقليديا أو حتى موضوعها جرائم الكترونية مادام أن المتابعة أو المصادرة..... ماديان لكن الإشكال بطرح أو يثار إذا تم مطاردة الجاني الكترونيا ما يسمى بالمطاردة الرقمية حال ارتكاب الجريمة بغرض القبض عليه [3] و هذا الإجراء ستنوء بتحمله جهود دولة واحدة، و هذا ما استشعره الفقه المقارن حجم المشكلة حين دعى إلى ضرورة القبول بالتعاون الدولي.[4]

كذلك يثار إشكال التفتيش عند وجود مبرر له فيتساءل عن حدوده و فيما إذا كان الحاسوب من ضمن محتويات المكان الذي يراد تفتيشه أم أنه هو بذاته يحتاج إلى إذن خاص.

المطلب الخامس : تعاون مزودي الخدمات رجال الضبط القضائي: مزود الخدمات[5]

الفرع الأول : مدى التزام مزودي الخدمات بسير المهنة:

---

[1] - 339.

[2] - كان التشريع الأمريكي قبل 2000/9/11 يمنع قيام جهات الاستدلال و التحقيق استخدام هذه البرمجيات و كان يتطلب للمراقبة الشخصية أن تكون تمت في إطار الاختصاص المكاني للمحكمة التي أصدرت الإذن، عمر محمد أبوبكر بن يونس ، مرجع سابق ، ص840- 841.

[3] - أثير هذا الموضوع عندما قامت المباحث الفدرالية الأمريكية بتعقب أحد الأشخاص عبر الشبكة حتى أمكنها رصد تحركاته و تحديد مكان ممارسة النشاط الإجرامي و انطلاقه من أي مزود خدمات و الحاسوب محل النشاط و تعلق نشاطه بزرع فيروس سماه LOVE RUGO و حدد مكان ممارسة النشاط الإجرامي بالفيليبين، عمر محمد أبوبكر بن يونس ، مرجع سابق ، ص842.
كذلك ابرم اتفاق بين شركة AOL .... عمر محمد أبوبكر بن يونس ، مرجع سابق ، ص847.

[4] - عمر محمد أبوبكر بن يونس ، مرجع سابق ، ص842.

[5] - حجازي، النظام القانوني للتجارة الالكترونية.

لا ينتمي مزود الخدمات إلى الطرائف التي يلزمهم القانون بسر المهنة – كالأطباء، المحامون... و غيرهم – ذلك أنه يجوز لرجال الضبط القضائي و سلطة التحقيق أن تلزمهم بتقديم المعلومات الخاصة بالمشتركين لديهم، و قد ذهب المشرع الفرنسي إلى أبعد من ذلك أي فيما يخص عدم التزام مزودي خدمات الانترنيت بسرية أعمال مهنتهم ما فرضه عليهم في القانون الصادر في 13 فيفري 2003في المادة 8 فقرة 1 من الالتزام بإفشاء أسرار الاتصالات عبر شبكة الانترنيت لرجال الضبط القضائي إذا كانت هذه المعلومات تفيد في كشف الحقيقة بخصوص تحقيق جنائي قادم.[1]

الفرع الثاني : التزام مزود الخدمات بالتعاون مع رجال الضبط القضائي:

تسمح غالبية التشريعات لرجال الضبط القضائي الذين يتولون و التحري أن يأمروا الأشخاص بتسليم ما تحت أيديهم من موضوعات و التي يطلب منها تقديمها كدليل، و هذا الاتجاه تبناه المجلس الأوربي بالنسبة للمعلومات المتواجدة داخل أنظمة الكمبيوتر التي هي في حوزة مزود الخدمات، حيث دعت لجنة الوزراء لهذا المجلس في توصيتها رقم 719 لسنة 2000 الخاص بحرية الاتصالات كل من ذوي خدمات الدخول و المسكنين بالمحافظة على بيانات مستعملي خدماتهم و ذلك تمهيد لطلب السلطات لتلك البيانات التي يحتمل أن تفيد كدليل في جريمة وقعت، كما يتعين على هؤلاء (أي مزودي الخدمات) المحافظة على سرية البيانات الشخصية المتعلقة بمستخدمي الشبكات حتى تلك التي تتعلق ممارسة الأعمال التجارية حيث تقوم إمكانية تقديمها أي تقديم تلك البيانات كدليل على التعاملات التجارية، طبقا لأحكام التوحيد الأوربي رقم 58 لسنة 2002، أما في القانون الأمريكي فقد تضمن قانون E.C.P.A حالات أجاز فيها لمزودي الخدمات الكشف الاختياري عن محتوى ملفات العملاء لديهم من هذا المجالات إذا تعلقت المعلومات بارتكاب جريمة.[2]

جاء في مقتضى المادة 29 من القانون الفرنسي المسمى بالأمن اليومي الصادر في 15 نوفمبر 2001 وجوب تسجيل البيانات المتعلقة بالاتصالات لمدة سنة و ذلك بغرض الحفاظ عليها كونها قد تفيد في بحث أو تقرير أو متابعة تحقيقات جنائية كما حدد ذات القانون البيانات التي يمكن تسجيلها لمدة سنة حيث هي لا تشمل محتوى الرسالة و لا الموضوع الذي رجع إليه المستخدم و إنما تشمل:

---

[1] **Nathalie DREYFUS, De la responsabilité des intermédiaires techniques : contrefaçon ou responsabilité civile ? Revue Communication Commerce électronique n° 1, Janvier 2007, Alerte 1**

[2] - شيماء عبد الغني ، مرجع سابق ، ص عبد الغني، ص 214.

عنوان الانترنيت بروتوكول
عناوين الرسائل الالكترونية المرسلة و المستقبلة
عناوين المواقع التي تم زيارتها.[1]
لكن هذا النص تم تعديله بمقتضى قانون الأمن الداخلي ليتوافق مع القانون الأمريكي (E.C.P.A)[2] حيث وسع من نطاق هذا الالتزام ليشمل محتوى الرسالة نفسها.
و قد كانت المادة 29 من قانون الأمن القومي تحظر الاطلاع عليها، مثلما فعل القانون الأمريكي حيث أجاز إلزام مزود الخدمات بالكشف عن محتوى الرسالة و عدم الاقتصار على الكشف عن أرقام الحساب و أسماء أصحابها و تاريخ مراسلاتهم كما يلزمه بالحفاظ على بيانات الاتصالات الالكترونية و من بينها ما تعلق بمحتوى الاتصال لمدة لا تزيد عن سنة و يلزمه بالكشف عنها بناءا طلب رجال الضبط القضائي لها بعد الحصول على إذن بذلك من النيابة العامة و بعد استئذان قاضي الحريات و الحبس[3].
بل إن بعض التشريعات كقانون الإجراءات الفرنسي أوجب على الجهات العامة و الأشخاص المعنوية الخاصة أن تضع تحت تصرف رجال الضبط القضائي البيانات التي تساعد في الكشف عن الحقيقة. حيث نصت المادة 1/60 ق إجراءات فرنسي [4] على أنه نلزم الجهات العامة و الأشخاص المعنوية الخاصة بناءا على طلب رجا ل الضبط القضائي بأن تضع تحت تصرفهم المعلومات التي تفيد في إظهار الحقيقة.
أما القانون الأمريكي بفعل ذلك التغير الذي طرأ عقب التشريعات مكافحة الإرهاب و فيها قانون *E.C.P.A* فإنه أجاز إطلاع رجال الضبط القضائي في إطار ما يقومون به من جمع الاستدلالات على البيانات الموجودة جوزه مزود الخدمات المتعلقة بمستخدمي شبكة الإنترنيت المتمثلة في:
المعلومات الشخصية الخاصة بالمشترك (اسمه، رقم هاتفه، عنوانه...)
المعلومات الشخصية الخاصة بالتعامل مع المشترك (كل من يتصل به أو يدخل معه في صفقة تجارية)
المعلومات المتعلقة بمحتوى الملفات و مضمونها.[5]

---

[1] - شيماء عبد الغني ، مرجع سابق ، ص عبد الغني، ص 211.
[2] - قانون حماية الحياة الخاصة في مجال الاتصالات الالكترونية.

[3] **Bruno P. LANGLOIS, La protection des marques sur internet : le législateur fédéral américain s'attaque à la cyber piraterie, Revue Gazette du Palais, 20 juillet 2000 n° 202, P. 29**

[4] - هذه المادة أدخلها قانون الأمن الداخلي سنة 2003.
[5] - شيماء عبد الغني ، مرجع سابق ، ص عبد الغني، ص 216.

و يتم إلزام مزودي الخدمات بالكشف عما لديهم من بيانات لرجال الضبط القضائي عن طريق:[1]

الأول: الإلزام بتقديم المعلومات

و ذلك عن طريق توجيه تكليف إلى مزود الخدمات من قبل رجال الضبط القضائي بتقديم معلومات شخصية خاصة بالمشترك و هذه الطريقة اعتمادها قانون الإجراءات الجنائية الأمريكي (أو الجزء 18 الفقرة 2703).

الثانـــي: صدور إذن بالتفتيـــش

على أساس إذن بالتفتيش يحصل عليه رجال الضبطية القضائية إذا تعلق الأمر ببيانات أو اتصالات مخزنة لدى مزود الخدمات قصد الاطلاع عليها تلك الاتصالات المخزنة و ضبطها.

الفرع الثالث : مدى حق رب العمل في مراقبة الاتصالات الالكترونية:

يتنازع هذا الطرح اتجاهات تزعمهما المشرع الأمريكي و المشرع الفرنسي و هما على طرفي نقيض.

فقد تعامل القضاء الأمريكي مع إشكالية مدى جواز أو حق.

الفرع الثالث : المراقبة الالكترونية للاتصالات عبر الاتصالات عبر الإنترنيت:

المراقبة أهم مصدر للتحري و التحقيق في الجرائم فهي وسيلة فاعلة للكشف الجرائم و تسمى في إطار جرائم المعاملات الالكترونية التجارية بالمراقبة الالكترونية *La cyber surveillances/to keepwatch* أو *surveillance électronique* و تعني مراقبة شبكة و الاتصالات باستخدام التقنية الالكترونية تجمع بواسطتها بيانات و معلومات عن المشتبه فيه لتحقيق غرض أمني يقوم بها مراقب مختصر ذو كفاءة تتماشى مع نوع الجريمة يحقق فيها [2] و لها أشكال مختلفة مع تطور التكنولوجيا الاتصالات أصبحت مفردات النصوص ذات معان تقليدية فإلى أي حد تصلح هذه النصوص، أساسا لتفتيش و ضبط شبكات الاتصال العالمية؟ و هل يمكن الاعتماد على هذه النصوص لإعطاء الصلاحية لمراقبة الاتصالات الالكترونية.[3]

رب العمل في أن يتدخل في جهاز الموظف ليراقب اتصالاته بطريق الكمبيوتر أو مطلع على..... معلومات أو بريد بإعطاء هذا الحق بل و بإمكانه أيضا ضبطه و تسليمه إلى الشرطة لكون أنه رب العمل في القطاع الخاص يمتلك أدوات العمل و يخصصها لمصلحة العمل، و الكمبيوتر أحد هذه الأدوات كما أنه إضافة لذلك لا ينشأ هنا لصالح العمل توقع مقبول لاحترام الحق في الحياة الخاصة، كما له الحق في المتابعة في التبليغ إلى جهات الشرطة و

---

[1] - شيماء عبد الغني ، مرجع سابق ، ص عبد الغني، ص 226- 227.

[2] - نبيلة مولاي، ص 69.

[3] - صابل فاضل، ص 283- 284.

التعاون معهم دون الحاجة إلى صدور إذن بالتفتيش للجهاز أما القضاء الفرنسي فإنه يغلب حق الموظف في الحياة الخاصة و كذلك القضاء الكندي يجيز لرب العمل أن يتنصت على المحادثات التلفونية التي تجرى بين المستخدمين في شركته و بين عملاء الشركة كون الأجهزة التليفونية مخصصة للعمل و قضت محكمة الاستئناف الكندية بصحة الدليل المستمد من تلك المراقبة و تذهب المحاكم الكندية إلى أكثر من ذلك و هو القول بمشروعية الدليل حتى و لو تم التسجيل بغير علم من تلك الطرفين. .[1]

بالرغم من أن المادة 03 من القانون المدني فأكد على الحق في الخصوصية و تعدد صورها المادة 36 من ذات القانون في 6 صور كما أوردت المادة 2858 الجزء المترتب على محالفة تلك النصوص و هو استبعاد الدليل عند استخدام أدوات العمل، و عليه ليس لرب العمل الحق في الاطلاع و لا مراقبة أو متابعة اتصالاته الشخصية التي تخص الموظف حال استخدامه جهاز العمل حيث المستخدم أو الموظف يتمتع بالحق في الحياة الخاصة في مكان و في أوقات العمل و أكد القضاء الفرنسي هذا عندما قضى بإدانة مدير دار شبكات وضع جهاز لتسجيل المكالمات التي يجربها الموظفون من مكان العمل و لا نزلاء الدار.[2]

المطلب السادس : الطبيعة الخاصة لإجراءات التحقيق في مجال التعاملات الالكترونية:

الفرع الأول : حرمة الحياة الخاصة للبيانات المعالجة آليا:

تعرضنا فيما سبق إلى أن البيانات المعالجة آليا لها مركز يحميه القانون و يحرم الاعتداء عليه، لكن إذا كان من متطلبات المتابعة أو التحقيق في جريمة ما فإن الآخر كذلك حيث استقر على أن الدخول لبيانات موجودة داخل النظام لا بد من أنه سبقه إذن بذلك من سلطة التحقيق و قد قضى بذلك التعديل الرابع للدستور الأمريكي حيث حمى البيانات المعالجة آليا من التداخل إليها عن بعد، مقيما التماثل بين الاقتحام المادي للمنازل و الاقتحام المعنوي للمعلومات. و هذا تحت ظل حماية الحق في الخصوصية الذي أكده التعديل الدستوري ذاته.[3]

الفرع الثاني : تجريم اعتراضي للاتصالات الالكترونية:

... الأساس الذي ترتكز عليه المعاملات الالكترونية التجارية شبكة الاتصالات... عنت تشريعات حديثة لإدخال نصوص خاصة تسري أحكامها على الاتصالات الالكترونية على غرار الاتصالات السلكية و اللاسلكية التي تعاقب على اعتراضاها دون إذن بذلك. كونه يعد انتهاك لحرية الحياة الخاصة.

---

[1] - شيماء عبد الغني ، مرجع سابق ، ص عبد الغني، ص 249- 250.

[2] - شيماء عبد الغني ، مرجع سابق ، ص عبد الغني، ص 237.

[3] - و ينسحب التعديل الرابع الدستوري الأمريكي على البريد الالكتروني و شمله أيضا بالحماية، حيث لم يجز الإطلاع أو التصنت أو التفتيش إلا بإذن قضائي مسبب وفقا للقواعد المستقر عليها في مجال التصنت و التفتيش، شيماء عبد الغني ، مرجع سابق ، ص عبد الغني، ص 242.

من هذه التشريعات القانون الجنائي الفيدرالي الأمريكي [1] حيث عاقب كل من قام باعتراض المراسلات الالكترونية مساويا بينها و بين الاتصالات السلكية بنصه على عقاب كل من اعترض أو حاول اعتراض أو حاول اعتراض أو ساعد غيره على أن يعترض أو يحاول اعتراض أي اتصال سلكي أو شفوي أو الكتروني.

و عاقب أيضا كل من أفشى أو حاول أن يفشى محتوى اتصال هاتفي أو الكتروني و عاقب أيضا على الدخول إلى معلومات مخزنة الكترونيا بدون تصريح أو تجاوزا لتصريح سابق، و عاقب على تعديل طريقة الدخول لصاحب الحق فيه و شدد العقوبة إذا توافر قصد خاص متمثل في الرغبة في الحصول على مزايا تجارية أو مادية.[2]

و الاعتراض عرفه القانون الأمريكي بأن كلمة "يعترض" تعني الحصول على محتوى الاتصال أو الالكتروني و ذلك باستعمال وسيلة الكترونية أو أي وسيلة أخرى.[3]

و عليه فإن مراقبة أو اعتراض الاتصالات الالكترونية يعد الدليل فيها باطلا إذا تمت دون إذن قضائي.[4]

الفرع الثالث : شروط تسجيل الاتصالات الالكترونية في القانون المقارن:

يشترط القانون الأمريكي لتسجيل الاتصالات الالكترونية استصدار إذن من القاضي المختص بناء على طلب من أحد أعضاء النيابة حددهم القانون الأمريكي بالموافقة على طلب تسجيل المحادثات الالكترونية الذي يقدمهم أحد رجال الضبط القضائي.[5]

و أجازت المحكمة الأوربية هذا الإجراء تطبيقا للمادة 8 من الاتفاقية الأوربية لحقوق الإنسان بشرط مادام محاطا بضمانات قانونية كما أحاطه بشروط في المادة 2/8 إذا كان هذا الإجراء ضروريا للوقاية من الجريمة تلخصت هذه الشروط في:[6]

وجوب صدور إذن من قاضي التفتيش

أن يكون الإذن الصادر مكتوبا و مفصلا

---

[1] - Mitle 18, part 1, chapitre 119, sec, 2511، شيماء عبد الغني ، مرجع سابق ، ص عبد الغني، ص 245، انظر أيضا:

Bruno P. LANGLOIS, La protection des marques sur internet : le législateur fédéral américain s'attaque à la cyber piraterie, Revue Gazette du Palais, 20 juillet 2000 n° 202, P. 29…

[2] - شيماء عبد الغني ، مرجع سابق ، ص عبد الغني، ص 246.

[3] - أكدت المحاكم الأمريكية أن الأصل أن الاتصال يكون اتصالا الكترونيا إذا لم يكن محمولا بواسطة الموجات الصوتية و لا يتضمن صوت إنسان حيث الإشارات الالكترونية أو الكهربائية التي لا تعتبر اتصالا سلكيا تعتبر اتصالا سلكيا بل تعتبر من قبيل الاتصالات الالكترونية، شيماء عبد الغني ، مرجع سابق ، ص عبد الغني، ص 248.

[4] - حدد القانون الأمريكي الجرائم التي يجوز فيها إصدار إذن باعتراض الاتصالات فيها الجرائم التي يعاقب عليها بالإعدام أو الجرائم التي عوقب عليها بالحبس لمدة سنة واحدة، شيماء عبد الغني ، مرجع سابق ، ص عبد الغني، ص 251- 252.

[5] -شيماء عبد الغني ، مرجع سابق ، ص عبد الغني، ص 252/ صابل فاضل، ص 285.

[6] - شيماء عبد الغني ، مرجع سابق ، ص عبد الغني، ص 257.

أن يكون الفعل الجرمي ..... في الجنايات و الجنح المعاقب عليها بعقوبة الحبس سنتين على الأقل.

و هذا الاتجاه أصبح اتجاها عالميا ففي فرنسا أدخل المواد من 100 إلى 7/100 من قانون الإجراءات الجنائية تتلخص مضامينها في جواز اعتراض الاتصالات البعدية بما في ذلك شبكات تبادل المعلومات ، أما في هولندا فإن القانون يجيز لقاضي التحقيق أن يأمر بالتنصت على شبكات الاتصالات الالكترونية عندما توصف الأفعال التي ضلع فيها المتهم بالجرائم الخطيرة.[1]

المبحث الثاني : التفتيش في بيئة التجارة الالكترونية

التفتيش في بيئة التجارة الكترونية

التفتيش ابتداء هو اختصاص منوط سلطة التحقيق و الممثلة في قاضي التحقيق و النيابة العامة حسب اختلاف التشريعات و هو إجراء منوط برجال الضبط القضائي على سبيل الاستثناء الوارد في القانون و هو إجراء يتطلبه التحقيق يقضي بتفتيش المتهم أو منزلة بضبط الأشياء المحصلة عن الجريمة[2] و ليس هو غاية في ذاته بل الهدف فيه البحث عن دليل يتعلق بالجريمة الواقعة سواء يغلق بالأشخاص أو الأماكن أي كانت طبيعة تلك الأماكن، و هو يختلف عن غيره من الإجراءات التي يمكن أن تنتابه معه كونه أحد إجراءات التحقيق.[3]

و تبعا للمفهوم التقليدي للتفتيش رأى البعض [4] أن هذا المفهوم غير منسجم مع بيئة المعاملات الالكترونية و بحاجة التجارة الالكترونية حيث هو يهدف إلى جمع الأدلة المادية حسب المفهوم التقليدي بينما بيئة التجارة الالكترونية و طبيعة المعاملات التجارية الالكترونية هي ذات طبيعة معنوية لا تتوافر لها صفة المادة مما يجعل من الصعوبة إن لم يكن من الاستحالة تطبيق فكرة التفتيش على الجرائم الواقعة على التجارة الالكترونية.

مدى صلاحية معاملات التجارة الالكترونية محلا لهذا الإجراء (التفتيش):

و في التقنين الإجرائي ليس غاية إنما هو للإثبات المادي يستهدف ضبط أشياء مادية تتعلق بالجريمة تفيد في الكشف عن الحقيقة أي الحصول على دليل مادي، و هذا الغرض بدوره ممكن

---

[1] - صايل فاضل ، مرجع سابق ، ص، ص 284.
[2] - نبيلة هروال ، مرجع سابق ، ص 79.
[3] - حجازي، مبادئ الإجراءات، 192- 193.
[4] - أسامة أحمد، حلال محمد، فاضل صايل، جرائم الحاسب، 264.

أن يثير إشكالا حول مدى اعتبار البحث عن أدلة جرائم في بيئة المعاملات الالكترونية التجارية نوعا من التفتيش كون البيانات المتعلقة بهذه المعاملات ذات كيان معنوي غير مادي محسوس.
هذا الإشكال دعى جانب من الفقه و التشريعات إلى أن تقف موقفان لاعتماد الإجراء.[1]
فأما الفريق الأول فقد رأى عدم موائمة قواعد التفتيش و الضبط و قصورها في قوانين الإجراءات الجنائية مع ما قد يتطلبه الوصول إلى جريمة في بيئة المعاملات الالكترونية، إن عادة ما يكون الغرض من التفتيش هو البحث عن شيء فإن أصحاب هذا الفريق قصور مصطلح شيء و ضرورة إكمال هذا البيان التشريعي بإضافة عبارة جديدة هي مادة معالجة بالحاسب.[2]
و على هذا الأساس اقترح فريق فريق من الفقه الفرنسي كعديل نصوص القواعد الناصة على أن التفتيش وسيلة لجمع الأدلة المادية ليصبح هدف التفتيش جمع بيانات معالجة آليا بالإضافة إلى جمع الأدلة المادية.
أما المشرع الإنجلو سكسوني فقد قابل جرائم الحاسب الآلي و من بينها جرائم التجارة الالكترونية بسن تشريعات جزائية قادرة من شأنها التصدي للظاهرة الإجرامية المعلوماتية.
و قد أفردت جانبا كبيرا من تلك التشريعات بحث مسألة التفتيش و الضبط ففي انجلترا مثلا أصدر قانونا..... بـــ "قانون إساءة استخدام الحاسب الآلي" 1990 نص على إجراءات تفتيش نظم الحاسب الآلي في جرائم الولوج غير المصرح به على أنظمة الحاسب الآلي، و التعديل غير المصرح به في نظام الحاسب الآلي بدون إذن طالما كان القصد من الولوج ارتكاب أفعال غير مشروعة، و يكون بإذن قضائي إذا كان الولوج مجرد من القصد الموصوف بالجرمي.[3]
أما المشرع الأمريكي فقد نظم إجراء التفتيش و الضبط في بيئة المعاملات الالكترونية من خلال القوانين الإجرائية الفيدرالية بأن جرائم الكمبيوتر في القسم 2000 *USL* 42.
أما فرنسا نظمت ذلك من خلال الاتفاقية الأوروبية لجرائم الأموال في المادة 19.[4]

أمـــا الفريـــق الثانـــي:

يستند إلى عمومية النص حيث يجري حمل ما تتضمنه التقنيات الإجرائية الجنائية في نصوصها عن إجراء التفتيش بعبارة أي شيء على المعنى الذي يحد نطاقها ليشمل البيانات الالكترونية بمختلف أشكالها أي كل البيانات المخزنة آليا في الأنظمة المعلوماتية و نموذج هذا

---

[1] - هشام رستم ، مرجع سابق ، ص، الجوانب الإجرائية، 65.
[2] - هشام رستم ، مرجع سابق ، ص 66/ نبيلة مولاي 79/ حجازي، مبادئ الإجراءات 198.
[3] - صابل فاضل 265 ، مرجع سابق ، - 266.
[4] - نص المادة بالفرنسية، نبيلة مولاي 79.

الاتجاه المشرع الكندي الذي أجاز في المادة 487 من القانون الجنائي الكندي إصدار أمر قضائي لتفتيش و ضبط أي شيء " Any Thing" طالما تتوافر بشأنه أسس و مبررات معقولة تدعو للاعتقاد بأن جريمة وقعت أو يشتبه في وقوعها أو أن هناك نية لاستخدامه في ارتكاب جريمة أو إنه يستبيح و يوفر دليلا على وقوع بجريمة و من شأن هذا النص إطلاق التفسير و التوسع في فهم و حكم الإجراء.[1]

فريـــق ثالـــث: يرى أن التشكيك في الطبيعة المادية لبيانات الالكترونية على نحو ما سبق شرحه ليس له ما يسوغه لاعتبارات تكنولوجية و أخرى قانونية يجب أن تراعي بين المعلومات من جهة و بين البيانات المعالجة آليا.

من جهة أخرى فالمعلومات ليست شيء مادي إنما هي عملية أو علاقة تقوم بين ذهن بشرى و بعض أنواع المثيرات، و هي مع تجسدها ماديا في وعاء أو ركيزة يمكن نقلها للغير بواسطتها هي من طبيعة معنوية و لا سبيل لأن يرد عليها تفتيش و ضبط، أما الثانية و هي البيانات المعالجة آليا فهي نبضات أو ذبذبات الكترونية و أشارت أو موجات كهرومغناطيسية قابلة لأن مسجل و تخزن على وسائط معينة يمكن نقلها و بثها و حجتها و استغلالها و إعادة إنتاجها كما تقديرها كميا و قياسها من حيث المبدأ، فهي ليست شيئا معنويا كالآراء و الأفكار بل سيء له وجود مادي في العالم الخارجي المحسوس. و يستشهد الدكتور هشام محمد فريد رستم – في معرض طرحه لهذا الرأي – بما وصفتها محكمة جنح بروكسل أشياء محسوسة و مادية "Tangibles et materirlles" و من ثم يصح قانونا أن يرد عليها التفتيش و الضبط [2] و عليه يعتبر تفتيش النظم الالكترونية المعالجة إجراء ينتدب..... التفتيش بمعناه القانوني و يخضع لأحكامه مع نوع من الخصوصية تتفق مع الجريمة المراد جمع الأدلة بشأنها و كذلك البيئة التي يتعامل معها رجال الضبط القضائي القائمين بذلك الإجراء.[3]

مع وجوب التقييد بحملة شروط تقرره قانونا.[4]

غير أن التفتيش معرفة معقولة من قبل الشخص القائم به (رحل الضبطية القضائية) بكيفية التعامل مع البرامج و ملفات البيانات المخزنة بالحاسب و كلمة السر و المرور اللازمين للدخول إلى النظام عندما يتعلق الأمر بالقيام بعملية ولوج إلى الأنظمة المعلوماتية التي تحويها لضبط ما يعدها صالحا لدليل يسوق الكشف عن الجريمة.[5]

---

[1] - هشام رستم ، مرجع سابق ، ص 67، نبيلة مولاي 80، حجازي مبادئ 198.
[2] - هشام رستم ، مرجع سابق ، ص 68- 69.
[3] - نبيلة مولاي 80.
[4] - راجع في بيان أحكام هذه الشروط نبيلة مولاي، ص 80- 81.
[5] - حجازي ، مبادئ الإجراءات 197.

أما عن الشروط التي يمكن أن يتطلبها هذا الإجراء فهي اختصارا تتعلق بتلك الضمانات الأساسية التي تحرص أغلبية التشريعات على إحاطة التفتيش بها يكون إجراء له صلة بالحريات الشخصية، بعضها موضوعي و آخر شكلي.

فأما الموضوعية فهي التي يقصد بها الشروط اللازمة لإجراء تفتيش صحيح و هي تحصر ثلاث شروط:[1]

سبب التفتيش في العالم الافتراضي:

أن يكون بصدد جريمة إنترنت وقعت بالفعل وقعت بالفعل (جنحة أو جناية)

نسبة هذه الجريمة إلى شخص أو أشخاص بصفتهم فاعلين أصليين أو شركاء في ارتكابها.

وجود قرائن دالة على أشياء أو أجهزة أو معدات معلوماتية تفيد كشف الحقيقة لدى المتهم المعلوماتي أو غيره.[2]

محل التفتيش:

مكونات الحاسب الآلي المادية و المعنوية

الشبكة و ما تتطلبه من مكونات

السلطة المختصة بالتفتيش

اتفاقية الجرائـــم (المجلس الأوربي) *The cyber crime convention*: [3]

الحمـــاية الإجرائيـــة:

القانون الجنائي هو أحد فروع القانون العام و هو يضم صنفين من القواعد القانونية:

القواعد الموضوعية و هي ما يصطلح عليها بقانون العقوبات و القاضية ببيان أحكام الجرائم و العقوبات المقررة لها.

و قواعد إجرائية لا تقل أهمية عن القواعد الموضوعية من حيث اعتماد الأخيرة عليها و هي ليست غاية في ذاتها، و إنما هي وسيلة لغاية تتمثل في حسن تطبيق القواعد الموضوعية للقانون الجنائي، و هي تشكل قانون ينظم وسائل التحقق من الجريمة و محاكمة مرتكبها و توقيع الجزاء عليه و منظم المحاكم الجنائية، و تبين إجراءات المتبعة في التحقيق و تنظيم سير

---

[1] - نبيلة مولاي 80- 91/ صابل فاضل 266 ، مرجع سابق ، - 277.

[2] - أنظر صابل فاضل ، مرجع سابق ، 270- 271- 272.

[3] - ابراهيم طارق إبراهيم الدسوقي ، مرجع سابق ، ص 334.

الدعوى[1] و غير ذلك مما يفيد في حفظ التوازن بين حق المجتمع في الحفاظ على تماسكه و أمنه و حق الأفراد في إيجاد ضمانات على عدم التعدي على حقوقهم.

المشروعيـــة فـــي مرحلـــة جمـــع الاستـــدلالات:

أقر المشرع اختصاصات معينة لمأمور الضبط القضائي عند البدء في أعمال التحقيق حرضا من الأول على سرعة ضبط الواقعة و عدم طمس الأدلة و ضياع معلم الجريمة و بالتالي صعوبة إقرار العدالة بشأنها، و هو ما يقتضي سرعة انتقال رجال الضبط القضائي إلى مكان ارتكاب الجريمة، و مباشر الاختصاصات المخولة لهم.[2]

و لعل أهم إجراءات الاستدلال ما نصت عليه المادة:[3]

الحماية الإجرائية القانونية للتجارة الالكترونية

إجراءات مواجهة جرائم التجارة الالكترونية

إجراء تفتيش نظم المعلومات.

التفتيش إجراء من إجراءات التحقيق يستهدف البحث عن الحقيقة في مستودع السر و هو يعد من أهم إجراءات التحقيق في كشف الحقيقة فهو في العادة يفضي للوصول إلى أدلة مادية تؤدي إلى نسبة الجريمة إلى المتهم، و حين يباشر التفتيش رجال الضبط القضائي فإنه يباشر إما على شخص المتهم و إما على مسكنه.[4]

و تناول المشرع الجزائري حق التفتيش في.....من قانون الإجراءات الجنائية.

و إذا كان إجراء التفتيش ذو أهمية بالغة كونه أكثر الإجراءات فائدة في إظهار الحقيقة فإن ذلك يقضي أن يباشره (أعضاء فريق) ضابط شرطة بسمات و قدرات متميزة غير الجريمة التي هو بصدد البحث عن دلائل عنها،تمكنه من القيام بأداء هذا الإجراء يشكل سليم تحقق الغاية منه إنما المساس بحق الأفراد، و لا يقوم بإجراء التفتيش إلا سلطة من السلطات المختصة بالتحقيق أو بأمر فيها فالتفتيش ليس بدليل و إنما وسيلة للحصول على الدليل.[5]

---

[1] - طارق إبراهيم الدسوقي ، مرجع سابق ، ص 342- 344.
[2] - طارق إبراهيم الدسوقي ، مرجع سابق ، ص 350- 351.
[3] - النص في ق إ ج ج.
[4] - طارق إبراهيم الدسوقي ، مرجع سابق ، ص 363.
[5] - طارق إبراهيم الدسوقي ، مرجع سابق ، ص ص469-464

كما أنه عند قيام بإجراء قانوني في إطار عمله كمأمور الضبطية القضائية لا بد أن يكون كما أنه عند قيامه بإجراء قانوني في إطار عمله كمأمور الضبطية القضائية لا بد أن يكون على علم بالطبيعة القانونية لهذا الإجراء حتى يؤدي بالشكل القانوني المحدد له حتى لا يصيبه البطلان.[1]

تفتيـــش نظـــم المعلوماتيـــة:

تفتيش نظم المعلوماتية يتم من خلال الوعاء الذي يحوي هذه النظم أي أجهزة الحاسب الآلي بمكونيه المادي *Hard War*، و المكون المنطقي *Soft War* بالإضافة إلى شبكات الاتصال، و في نطاق تنفيذ مأمور الضبط القضائي لإجراء التفتيش في المعلوماتية لضبط جرائم متعلقة بالتجارة الالكترونية يثار تساءل هام عن مدى خضوع أجهزة الحاسب الآلي للتفتيش.[2]

التفتيـــــش:

تبعا لطبيعة التفتيش إجراء التفتيش أولا و لخصوصية الجرائم الواقعة في التجارة الالكترونية نجد أن المشرد الفدرالي الأمريكي حول تفتيش و ضبط الحاسوب يضع أجزاء لمقياس فاصل. بعد تفتيش نظم الحاسب و الانترنيت من أخطر مراحل الإجراءات الجنائية كون محل التفتيش في جرائم المعلوماتية هو الحاسوب و الشبكات و هما محل استفسار متزايد حيث المرشد الفدرالي لضبط و تفتيش الحاسوب و الحصول على أدلة الكترونية في التحقيقات الجنائية المطور عام 2001 و 2003 و ميز فيه بين مرحلتين:[3]

مرحلة ضبط و تفتيش الحاسوب دون إذن تفتيش

مرحلة ضبط و تفتيش الحاسوب و بوجود إذن تفتيش

ثم إن بعض التشريعات كالتشريع الجنائي الكندي يذهب إلى تفضيل أو تخصيص لموضوع التفتيش في كل حالة على حده كما هو الشأن في الإجراءات المتبعة في جريمة العدوان على العلامات التجارية (القسم 487 من قانون العقوبات الكندي).

و قد تضمنت المادة 2 من التوصية الأوربية بشأن الإجراءات الجنائية المتعلقة بتكنولوجيا المعلومات – إجابة عن تساؤل عن مدى إمكانية اعتبار الحاسوب تشمله قواعد الخصوصية و يدرج ضمنها أم أنه يعد من قبيل محتويات المكان الذي يوجد فيه فيطاله إجراء التفتيش، حيث

---

[1] - طارق إبراهيم الدسوقي ، مرجع سابق ، ص 372.

[2] - طارق إبراهيم الدسوقي ، مرجع سابق ، ص 379.

[3] - عمر محمد أبوبكر بن يونس ، مرجع سابق ، ص854.

نصت على أنه يجب أن تسمح قوانين الإجراءات الجنائية لسلطات التحقيق بتفتيش نظم الحاسوب و مصادرة البيانات بذات الأوضاع المقررة في نظم التفتيش و الضبط التقليدية.[1]
كما أعطى المشرع البلجيكي عام 2000 تعديلا لقانون التحقيق الجنائي أعطى بموجبه صلاحية لقاضي التحقيق بإصدار إذن تفتيش لنظم المعلومات.
غير أن بمراعاة بمبدأ الغاية من التفتيش مميزا البعض في هذا الإجراء حيث إذا اعتبر الحاسوب جزء من المكان الذي أذن بتفتيشه، شمل إذن التفتيش تخصيصا للجهاز كون الحاسوب متميز عن المحتويات العادية لمنزل حيث الصيغة العامة لا تكفي بل يجب أن يتضمن إذن التفتيش تحديدا دقيقا للحاسوب المراد تفتيشه [2] و عدد الأجهزة المراد تفتيشها [3] و كلما زاد تخصص في إذن التفتيش كان بالإمكان أكثر تطبيق القواعد العامة للتفتيش الواردة في قانون الإجراءات الجنائية من حيث تبرير القيام به و الالتزام بغاياته و عدم تعارض الإجراء مع الحقوق المقررة دستوريا، و حتى جاء إذن التفتيش عاما جاء به عن الغرض المخصص له مما يجعل مسألة التجاوز في التفتيش قائمة و يقع الإجراء تحت طائلة البطلان.[4]
إن التفتيش أحد أقوى الإجراءات الجنائية المقررة للتصدي للظاهرة الإجرامية و بتطوراتها الحديثة، هذا التطور شكل إشكالا و طرح تساؤلات عدة حول مدى كفاية القواعد القانونية للانطباق على منهج التفتيش كإجراء أولي عبر الإنترنيت على جرائم الإنترنيت سعيا وراء الحصول على أدلة في جرائم افتراضية أو إمكانية تقييم لمنهج التفتيش لكل في قانون الإجراءات الجنائية على أساس تغيير المعطيات (معطيات الظاهرة الإجرامية التقليدية) التي استند عليها المشرع أثناء تقريره لقواعد العامة التقليدية و حركية التطور العلمي و التقني و التكنولوجي بالأخص المجال التجاري الذي بدوره استفاد من تقنية المعلوماتية و لعل تضرر بذات التقنية بمثل ما استفاد.
أما عن محل التفتيش في جرائم التجارة الالكترونية و الجرائم المعلوماتية عموما فإنه يقع على مكونين هما:[5]
القطع الصلبة *Hard ware* و البيانات *Rata* و القيمة الاستردادية فيها متمثلة في المعلومات و هما يشكلان وحدة واحدة لا تعمل واحدة دون أخرى.

---

[1] - عمر محمد أبوبكر بن يونس ، مرجع سابق ، ص854.
[2] - ينبغي أن يكون إذن التفتيش دقيقا ليكون مبررا القيام بإجراء التفتيش، و يحوي كيفية و مكان حدوثه و تحديد القطع التي هي محل تفتيش و البرمجيات التي يحويها الجهاز و كذلك السجلات و البيانات المخزنة في هيئة الكترونية أو مغناطيسية مشفرة أو بطريقة الوسائط المتعددة، و كل المرئيات المصورة المخزنة في الحاسب (صور عن توقيع مزور، برمجيات لفتح كلمات دخول، فك شفرة برنامج...)، عمر محمد أبوبكر بن يونس ، مرجع سابق ، ص862- 863.
[3] - عمر محمد أبوبكر بن يونس ، مرجع سابق ، ص854- 855.
[4] - عمر محمد أبوبكر بن يونس ، مرجع سابق ، ص ص863-865.
[5] - عمر محمد أبوبكر بن يونس ، مرجع سابق ، ص865.

و يطال التفتيش ملحقات الحاسب التي لها علاقة بشبكة الإنترنيت.

فحـــص نظـــام الأمـــن المـــادي:

إذا كان على سبيل المثال الغرض من التفتيش تقصي جريمة مالية واقعة في مؤسسة تجارية فإن البحث يبدأ النظام الأمني لإمكانية التوصل إلى كيفية الاختراق أو برمجيات الاختلاس أو النصب للكشف عن العلاقة بين مؤلفها و بين الجريمة المرتكبة.[1]

فحـــص نظـــام التشغيـــل:

و يتم عن طريق فحص ملفات النظام، و هو ما يمكن من معرفة حركة الحاسب أو الخادم و يفيد هذا الإجراء في الكشف أيضا عن السرقات التي يمكن أن تم في المعالجات، و يفيد أيضا في الكشف عن هوية صاحب الجهاز أو مستخدمه في الجريمة.

فحـــص البرمجيـــات:

عمل البرمجيات ينصب حول العمل على استحداث معالجة آلية للبيانات و تحقق البرمجيات "قيمة استردادية بما تحويه من بيانات يمكن أن يتم معالجتها لكي تمدنا بمعلومة تمثل الغرض النهائي من المعالجة الآلية للكل"[2]، و القيام بفحص هذه البرمجيات يساهم في الكشف عن بعض الجرائم التي أشرنا لها سلفا و أكثرها خطورة مثل جرائم الاختراق و الدخول غير المشروع إلى (نظم المعالجة الآلية للبيانات) مواقع التجارة الالكترونية[3]

المطلب الأول : الخصائـــص التـــي تمييز التفتيـــش:

تقيم أحكام القضاء التماثل بين مراسلات البريد الالكتروني و المراسلات البريدية العادية إذ تحكم بعدم جواز الإطلاع عليه إلا بإذن صاحبه ما لم يصدر إذن قضائي بذلك مصاحب البريد الالكتروني يتمتع بالحق في جريمة الحياة الخاصة فيما يتواجد فيه من معلومات و بيانات فتلك حقوق تدخل ضمن محمية القانون و الدستور في التشريعات المقارنة من حق للخصوصية و على سبيل المثال قضى في كندا ببطلان الدليل المستمد من البريد الالكتروني لأحد الأشخاص دون موافقة الأخير.

---

[1] - عمر محمد أبوبكر بن يونس ، مرجع سابق ، ص866.

[2] - عمر محمد أبوبكر بن يونس ، مرجع سابق ، ص867.

[3] - عمر محمد أبوبكر بن يونس ، مرجع سابق ، ص867.

و قضت محكمة كندية ببطلان الدليل في قضية تجارة غير مشروعة عندما طعن المتهم بتهمة تقليد البرامج[1] ببطلان الدليل استنادا إلى أن رجل الضبطية القضائية قد خالف حق المتهم في حرية حياته الخاصة.

و قد أسست المحكمة حكم بالأسباب التالية:[2]

بطلان إجراء التفتيش لعدم وجود إذن مسبق

التعسف في إجراء التفتيش (بفتح ملفات ليس لها علاقة بالتهمة الموجهة للمتهم)

فتح البريد الالكتروني من قبل رجل الضبطية القضائية حيلة تمس بحق المتهم في التوقع المعقول للحياة الخاصة

الإجراء بحد ذاته يمثل مخالفة للمادة 02 من ميثاق الحقوق و الحريات الكندي.

الفرع الاول : مدى جـــواز التفتيـــش لضبـــط المعلومـــات:

أجازت التشريعات الحديثة تفتيش الأجهزة الالكترونية لضبط المعلومات – التي تفيد في كشف الحقيقة – المتواجدة فيها ولفرض الطبيعة المعنوية لمعلومات قواعد خاصة للتفتيش لضبط الأشياء المادية.

و لذا نجد الاتفاقية الأوربية في شأن جرائم السبر بحق الدول الأعضاء في تفتيش أجهزة الحاسب الآلي في إطار الإجراءات الجنائية حيث نصت المادة 19 من القسم الرابع على أن كل دولة طرف من حقها أن تسن من القوانين ما هو ضروري لتمكين السلطات المختصة أن تقوم بتفتيش أو الدخول إلى:

نظام الحاسب الآلي أو جزء منه أو المعلومات المخزنة به.

الوسائط التي يتم تخزين معلومات الحاسب الآلي بها.[3]

كما أكد المجلس الأوربي في توصية صادرة عنه رقم 13 (95) *R* على أنه يتعين مراجعة القوانين في مجال الإجراءات الجنائية لسماح باعتراض الرسائل الالكترونية و تجميع البيانات المتعلقة بتداول المعلومات في إطار التحقيق في جرائم ماسة بسلامة و سرية الاتصالات أو أنظمة المعلوماتية.

و تضمنت أيضا أنه يتعين السماح لسلطات التحقيق و الاستدلال بالتزوير بالوسائل الفنية الحديثة التي تمكنهم من تجميع المعلومات الضرورية لتحرياتهم و تحقيقاتهم.[4]

---

[1] - تتلخص وقائعها في قيام مأمور الضبط القضائي بتفتيش جهاز الحاسب الآلي الخاص بالمتهم و أثناءه دخل على البريد الالكتروني و وجد به رسائل جنسية خاصة بقصر يحظر القانون حيازتها على الأشخاص، شيماء عبد الغني ، مرجع سابق ، ص عبد الغني، ص 261.

[2] - شيماء عبد الغني ، مرجع سابق ، ص عبد الغني، ص 262.

[3] - شيماء عبد الغني ، مرجع سابق ، ص عبد الغني، ص 270.

[4] - شيماء عبد الغني ، مرجع سابق ، ص عبد الغني، ص 269.

الفرع الثاني : اختلاف تفتيش و ضبط المعلومات المخزنة عن الاتصالات المباشرة:

نصت التوصية13-95-*R* الصادرة عن المجلس الأوربي على أنه يجب إقامة التفرقة و التمييز بين تفتيش المعلومات المخزنة و ضبطها و بين اعتراض تلك المعلومات عند انتقالها، و هذا واضح من خلال ما يتبع من خطوات كل إجراء فاعتراض الاتصالات على الخط يتم وضعها تحت التنصت و تسجيلها. و هذا الإجراء يحتاج لإجراءات أكثر صرامة فيها صدور إذن من القاضي الجزائي بناءا على طلب من النيابة العامة وفقا للقوانين المقارنة، بينما التفتيش بغرض ضبط المعلومات المخزنة (بما فيها المحادثات التي انتهت) يتميز بقواعد أقل طرافة فيكتفي بإذن من النيابة العامة.[1]

نصت إحدى التوصيات (رقم 02) المجلس الأوربي على أنه يجب أن تسمح قوانين الإجراءات الجنائية لسلطات التحقيق أن تقوم بتفتيش أنظمة الكمبيوتر و أن تضبط المعلومات وفقا لشروط معينة و يتعين إخطار الشخص المسئول عن النظام بنوع المعلومات التي تم ضبطها، كما يجب أن تتاح له وسائل الطعن القضائي ما يتاح في غير ذلك من حالات التفتيش.

و عينت التوصية 13- 95-*R* بالنص على أنه تعتبر البيانات المعالجة آليا بالكمبيوتر في حكم المستندات التقليدية، و يسري على تفتيشها و ضبطها ما يسري على غيرها من تفتيش و ضبط تلك المستندات.[2]

الفر ع الثالث : إلــزام مزودي الخدمــات بالتعــاون مــع المحقــق:

تلزم التشريعات الحديثة المقارنة مزودي الخدمات بالتعاون مع المحقق بالإضافة إلى إلزامهم بالتعاون مع رجال الضبط القضائي.

و نصت التوصية رقم 13-95-*R* الصادرة عن المجلس الأوربي على وجوب فرض التزام على مزودي الخدمات حال تأدية خدماتهم للجمهور، أن يقدموا لسلطة التحقيق المعلومات اللازمة لتحديد هوية مستعمل الشبكة.

و نصت المادة 20 من الباب الخامس للاتفاقية الأوربية لجرائم السيبر أنه لدول الأعضاء أن تلزم مزودي الخدمات في حدود ما تسمح به وسائل الفنية المتاحة أن يقوم بـــ:[3]

تجميع أو تسجيل البيانات بالوسائل الفنية المناسبة.

يتعاون مع السلطة الوصية في تجميع و تسجيل البيانات المتعلقة بحركة التداول في الوقت الحقيقي المتعلقة بالتي تجرى على إقليمها الكترونيا، هذا التعاون هو واجب في مرحلة المحاكمة

---

[1] - شيماء عبد الغني ، مرجع سابق ، ص عبد الغني، ص 270.
[2] - شيماء عبد الغني ، مرجع سابق ، ص عبد الغني، ص 271.
[3] - شيماء عبد الغني ، مرجع سابق ، ص عبد الغني، ص 272.

حسب التشريع الأمريكي الذي يلزم مزودي الخدمات بتقديم ما لديهم من معلومات تخص المشتركين و المتعاملين معهم، هذا الإلزام معلق على جملة من الشروط هي:[1]

وجود تحقيق جنائي

وجود ما يدعوا عن كون كشف هذه المعلومات يفيد في إظهار الحقيقة، و يمتد اختصاصها عند إصدار أمر التعاون إلى خارج دائرة اختصاصها المحلي مادمت المحكمة مختصة أصلا بمحاكمة المتهم عن الجريمة.[2]

التعـــاون الـــدولي فـــي مجـــال تفتيـــش أنظمـــة المعلوماتيـــة:

عنصر مهم.[3]

صعوبات تتعلـــق بالتعاون الدولي في مجال تحقيـــق الجرائم الالكترونية:

عنصر مهم.[4]

المطلب الثاني : القواعد التي تنظم التفتيش و الاعتراض و التسجيل في مجال التعاملات الالكترونية:

الفرع الاول : تفتيش النظام بناء على إذن:

لا تجيز التشريعات المقارنة تفتيش أجهزة الكمبيوتر إلا بناء على إذن كأصل عام لكن هناك استثناءات لهذا الأصل.

01- شروط إذن التفتيش في المواد الالكترونية:

لها جملة شروط.[5]

ا/ خطـــورة الجريـــمة:

تشترط الكثير من التشريعات لصحة التفتيش كالقانون الفنلندي الذي يشترط في حصول إجراء التفتيش أن تكون الجريمة معاقبا عليها بالحبس لمدة تزيد على ستة أشهر و حذا حذوه المشرع الهولندي و كذا الاتفاقية الأوربية لحقوق الإنسان.

ب/ جديـــة التحريـــات:

قد يكون هذا الشرط ضابطا لحقوق يخشى عليها من تهددها إجراءات التحقيق ذلك أنه يلزم أن يصدر الإذن بالتفتيش بناء على تحريات جدية، و لا يصدر إلا بناء على دلائل كافية حسب

---

[1] - شيماء عبد الغني ، مرجع سابق ، ص عبد الغني، ص 273- 274.
[2] - شيماء عبد الغني ، مرجع سابق ، ص عبد الغني، ص 273.
[3] - شيماء عبد الغني ، مرجع سابق ، ص عبد الغني، ص 274- 278.
[4] - شيماء عبد الغني ، مرجع سابق ، ص عبد الغني، ص 278-279.
[5] - شيماء عبد الغني ، مرجع سابق ، ص عبد الغني، ص 281- 282.

الدستور الأمريكي في التعديل الرابع فيه و كذلك القبض و هذا ما أكدته قواعد الإجراءات الجنائية الأمريكية الفدرالية في الفقرة 41/جـــ[1].

جـــ/ التحديـــد فـــي الإذن:

يعد هذا الشرط دقيقا بالنظر إلى الغاية من الإجراء ذاته حيث محل التفتيش ذو طبيعة متميزة في هذه الجرائم كما أنه معقد و لكنه يجب على السلطة التي تباشر الإجراء أن لا تتجاوز حدود الإذن كأن ينص الإذن على ضبط المعلومات فيضبط الجهاز ذاته.

و لا يخفى ما يثيره هذا الشرط من صعوبات كون شرط تقني بالدرجة الأولى.[2]

02- مجـــال الإذن بالتفتيـــش:

ينصرف الإذن بالتفتيش مسكن المتهم أو محل عمله إلى كل ما يتواجد في المسكن أو مقر العمل و تفتيش كل أجزاءه مادام أن ذلك يفيد في كشف الحقيقة و من حق رجل الضبط القضائي تفتيش أجهزة الكمبيوتر الموجودة داخل المسكن و مكان العمل. [3] و أخذ القضاء في أمريكا بصحة تفتيش الصناديق المغلقة المتواجدة في المكان الذي ورد عليه التفتيش لكون القواعد العامة تسمح بتفتيش الأشياء المغلقة إذا كان الإذن بالتفتيش صادرا بخصوص المكان الموجودة به الأشياء و ليس هناك ما يمنع من صدور إذن بالتفتيش مقتصرا على تفتيش الكمبيوتر فقط دون بقية أجزاء المسكن أو محل العمل أو الشخص المتهم إذا كانت التهمة الموجهة للمتهم لها علاقة بجرائم معاملات التجارة الالكترونية.[4]

و أشير في هذا الإطار طرح إشكال متعلق بتحديد الإذن و مجاله فيما ارتبط أي ملف من الملفات يخضع للتفتيش و هل يتطلب فتح كل ملف إذنا قضائيا مستقلا على حده و السبب في طرح هذا الإشكال الذي تباينت الأحكام القضائية في تقريره هو أن فتح كل الملفات فيه تهديد لحق خصوصية المقرر دستوريا حيث الكمبيوتر بملفاته يحوي الكثير من المعلومات التي تتعلق بالحياة الخاصة لصاحبه و هو ما يعني الاعتداء على حق الأفراد.[5]

03- قواعد تنفيذ إذن التفتيش في المواد الالكترونية:

---

[1] Bruno P. LANGLOIS, La protection des marques sur internet : le législateur fédéral américain s'attaque à la cyber piraterie, Revue Gazette du Palais, 20 juillet 2000 n° 202, P. 29…

[2] - راجع في هذه الصعوبات شيماء عبد الغني ، مرجع سابق ، ص عبد الغني، ص 284- 288.

[3] - شيماء عبد الغني ، مرجع سابق ، ص عبد الغني، ص 289.

[4] - شيماء عبد الغني ، مرجع سابق ، ص عبد الغني، ص ص 289-294.

[5] - شيماء عبد الغني ، مرجع سابق ، ص عبد الغني، ص 290.

يخضع إذن التفتيش في المواد الالكترونية لقواعد عدة منها ما هو مستمد من القواعد العامة مع تطويعها لتتلاءم مع طبيعة المواد الالكترونية و فيها ما روعي فيه خاصية المادة المعلوماتية.[1]

أ/ تفتيش النظام الرئيسي و الأنظمة المتصلة به في الداخل:

من التعقيد بمكان الوصول إلى أحكام ضابطة لهذا العنصر ذلك أنه يثار حوله تساؤل مفاده هل يمتد تفتيش كمبيوتر معين إلى الأجهزة المرتبطة في داخل البلاد ؟ و هل يمكن تفتيش الأنظمة المتصلة بنظام المأذون بتفتيشه إذا تواجدت في دائرة اختصاص مختلفة ؟.[2]

هذه التساؤلات طرحتها مشكلات قانونية كشفت عنها ممارسة الإجراء ذاته حيث أشكل على سلطة التفتيش إذا تعلق الإذن بتفتيش شركة تجارية ما هل يمتد هذا الإذن إلى فروع الشركة الأخرى، و هل يمتد الإذن بالتفتيش إلى تفتيش جميع أنظمة الشركة أم يقتصر على الأنظمة الكائنة في مكان معين.

بعض القوانين المقارنة[3] تسمح بامتداد التفتيش إلى الأجهزة المرتبطة لمعرفة ما يفيد في كشف الحقيقة، و قضت المحاكم الأمريكية بصحة الدليل عند تفتيش الشبكة إذا تم ضبط بيانات خارج دائرة اختصاص المحقق الذي أصدر إذن التفتيش.

أما القانون الكندي فقد وضع نطاقا خاصا تضمنه القانون الجنائي الكندي متعلق بتفتيش الكمبيوتر في المادة (a) (2,1) 487 *Subsection* بمقتضى تعديل 08 مارس 1996 بنصها يمكن أنه "للقائم بتفتيش النظام وفقا لأحكام هذا الفصل أن يقوم بتفتيش أجهزة الكمبيوتر الأخرى المتواجدة في نفس المكان هذا الفصل أن يقوم بتفتيش أجهزة الكمبيوتر الأخرى المتواجدة في نفس المكان أو في نفس المبنى الذي صدر بخصوصه إذن بتفتيش كمبيوتر متواجد فيه بضبط و تفتيش البيانات التي تحتويها تلك الأجهزة أو البيانات المتاحة لهذه الأجهزة".[4]

أما في فرنسا فقد سمح منطوق المادة 1/18 من قانون الأمن الداخلي رقم 2003/239 الصادر في 18 مارس 2003 لرجال الضبط القضائي أن يدخلوا في الجهاز الرئيسي للبيانات التي تهم عملية البحث و التحري، و أجازت لرجال الضبط القضائي "أن يدخلوا عن طريق الأنظمة المعلوماتية المثبتة في الأماكن التي يتم فيها التفتيش على البيانات التي تهم التحقيق و المخزنة

---

[1] - شيماء عبد الغني ، مرجع سابق ، ص عبد الغني، ص 293.
[2] - شيماء عبد الغني ، مرجع سابق ، ص عبد الغني، ص 296.
[3] - ألمانيا ، النمسا ، فنلندا ، النرويج و الولايات المتحدة الأمريكية.
[4] - شيماء عبد الغني ، مرجع سابق ، ص عبد الغني، ص 299.

في النظام المذكور أو في أي نظام معلوماتي آخر مادمت هذه البيانات متصلة في شبكة واحدة مع النظام الرئيسي أو يتم الدخول إليها أو تكون متاحة ابتداء من النظام الرئيسي".[1]

كما سمحت الاتفاقية الأوربية لجرائم السيبر 2001 للدول الأعضاء أن يمتد نطاق التفتيش الذي محله جهاز واحد إلى غيره من الأجهزة المرتبطة به إذا كان يتواجد به معلومات تفيد الكشف عن الحقيقة و كانت الحالة هذه ..... بالاستعجال و ذلك في المادة 19 من القسم الرابع بنصها على أنه "من حق السلطة القائمة بتفتيش الكمبيوتر المتواجد في دائرة اختصاصها أن تقوم – في حالة الاستعجال – بمد نطاق التفتيش إلى أي جهاز آخر إذا كانت المعلومات المخزنة يتم الدخول إليها من الكمبيوتر الأصلي محل التفتيش".[2]

بينما تقتصر تشريعات أخرى حدود التفتيش و أثر الإذن على الأجهزة الموجودة في مكان محدد و دونما أن يمتد أثر ذلك الإذن إلى الأجهزة المرتبطة به كالتشريع البلجيكي و السويسري.[3]

ب/ مدى جواز تفتيش النظام الموجود خارج دائرة الاختصاص الإقليمية:

أثارت اللجنة الأوربية للمشكلات الجنائية التابعة للمجلس الأوربي في توصيتها رقم 89/9 حول علاقة الجريمة بالحاسب الآلي.

مسألة ابتداء إجراء التفتيش إلى النظام الرئيسي و الأنظمة المتصلة به في الخارج يقولها "التفتيش و الضبط و الإجراء ..... الأخرى تقع على إقليم دولة أخرى تعتبر غير مشروعة، إلا إذا كان القانون الدولي يجيزها".[4]

لكن و في تاريخ لاحق عرف ذات المجلس الأوربي في التوصية رقم 95/13 المتعلقة بمشكلات الإجراءات الجنائية المرتبطة بالتكنولوجيا.

"المعلوماتية – عرف خبراء مجلس التفتيش يقولهم بتوافر التفتيش في إقليم دولة أجنبية إذا توافرت ..... بين أفعال سلطات التحقيق في بلد معين و بين عمل جهاز كمبيوتر يتواجد في الخارج".[5]

و من الواضح أن المسألة أعقد من ذلك كون عدم وجود قانون جنائي معين أو موحد يحكم المعاملات الالكترونية، بل إن تعدد القوانين الجنائية التي تطبق عليها بتعدد المشرعين المعينين

---

[1] - النص الأصلي بالفرنسي عند شيماء عبد الغني ، مرجع سابق ، ص عبد الغني، ص 299.

[2] - النص الأصلي بالفرنسية عند شيماء عبد الغني ، مرجع سابق ، ص عبد الغني، ص 300.

[3] - لا يشترط في حالة التلبس الحصول على إذن سبق عن إجراء التفتيش على الجهاز الحاسب حيث تقوم إمكانية تفتيش حتى الأجهزة المرتبطة به، شيماء عبد الغني ، مرجع سابق ، ص عبد الغني، 301.

[4] - شيماء عبد الغني ، مرجع سابق ، ص عبد الغني، ص 304.

[5] - شيماء عبد الغني ، مرجع سابق ، ص عبد الغني، ص 304.

بتنظيم و استغلال شبكة الانترنيت، باعتبار أن القانون الجنائي يتعلق بسيادة الدولة و هذا يكمن الإشكال.[1]

إذا كان إجراء تفتيش الحاسب و الأجهزة المتصلة به يثير بعض التعقيدات فإن هذا التعقيد يكون أكثر تعقيدا عندما تسمح بعض التشريعات بانتداب إجراء التفتيش خارج نطاق إقليم الدولة أي أنها تسمح بتفتيش الأنظمة المتصلة بالحاسب أو الجهاز و لو كانت موجودة خارج إقليم الدولة و هذا فعلا ما ترتكز عليه المبادلات التجارية الالكترونية حيث يكون هناك بالضرورة امتداد للشركة التجارية أو المؤسسة التجارية بوجود فروع لها بالخارج فالأجهزة ترتبط ببعضها البعض أو أنها ترتبط بقاعدة بيانات، و نذكر على السبيل المثال هذه التشريعات:[2]

صدر عن المجلس الأوربي توصيات أجازت امتداد إجراء التفتيش إلى الشبكة المتصل بها حتى تنص

التوصية رقم 13 الصادرة سنة 1995 المتعلقة بالمشكلات القانونية لقانون الإجرائية المتصلة بتقنية المعلومات على أنه [3] "لسلطة التحقيق عند تنفيذ تفتيش المعلوما ت وفقا لضوابط معينة أن تقوم بمد مجال تفتيش كمبيوتر معين يدخل في دائرة اختصاصها إلى غير ذلك من الأجهزة مادامت مرتبطة بشبكة واحدة و أن تضبط البيانات المتواجدة فيها، و..... أنه من الضروري التدخل الفوري للقيام بذلك".

أما التوصية رقم 17 فنصت على أنه يمكن أن يمتد نطاق تفتيش الكمبيوتر إلى النظام المتواجد في الخارج، إذا كان من الضروري اتخاذ إجراءات عاطلة في هذا الشأن و يتعين أن يوحد أساس قانوني لامتداد مجال هذا النوع من التفتيش، حتى لا يشكل ذلك الإجراء مخالفة لسيادة دولة أجنبية، لذلك فإنه من الضروري الحصول على موافقة الدولة عند التفتيش إلى نظام يتواجد في إقليمها.[4]

أما المادة 18 فقد نصت على أنه:

"من الضروري إدخال إجراءات تتم بالاستعجال تخول سلطات البحث و التحقيق أن تطلب من سلطات أجنبية أن تقوم بتجميع الأدلة بشكل عاجل، لذا يجب تخويل السلطات المطلوب إليها أن تقوم بتفتيش نظام الكمبيوتر و ضبط البيانات بغرض نقل تلك الإجراءات لاحقا للجهة الطالبة، و يتعين أن يكون من سلطة الجهة المطلوب فيها أن تقوم بتزيد الجهة الطالبة بالمعلومات المتعلقة بحركة المراسلات الالكترونية و أن تقوم باعتراض اتصالات معينة أو تقوم بتحديد مصادرها،

---

[1] - جميل عبد الباقي الصغير ، مرجع سابق ، ص، الجوانب الإجرائية لجرائم المتعلقة بالانترنيت، ص 43.

[2] - شيماء عبد الغني ، مرجع سابق ، ص عبد الغني، 302- 303.

[3] - نص المادة بالفرنسية، شيماء عبد الغني ، مرجع سابق ، ص عبد الغني، ص 302.

[4] - نص المادة بالفرنسية، شيماء عبد الغني ، مرجع سابق ، ص عبد الغني، ص 303.

و لتحقيق هذا الغرض يتعين إيجاد من الوسائل ما يسمح بالمساعدة القضائية في هذا الخصوص".[1]

أما قانون الإجراءات الجنائية الهولندي فقد أجاز في المادة 125 منه تفتيش الأجهزة المتواجدة على إقليم الدولة إلى الأجهزة الأخرى المتصلة بها في دول أخرى.

كما سمحت للقاضي أن يطلب من الشاهد أن يدلي بأقوال عند معلومات تتواجد عن خارج البلاد.[2]

أما القانون الفرنسي رقم 239 سنة 2003 بشأن الأمن الداخلي الصادر في 18 مارس سنة 2003 فقد أجاز في المادة 2/18 منه لرجال الضبط القضائي أن يقوموا بتفتيش النظام المتصل بالجهاز و لو كان متواجد خارج الإقليم بنصها "إذا كانت البيانات مخزنة في نظام معلومات يقع في خارج إقليم الدولة، فإنه يجوز لرجال الضبط الدخول إلى هذه البيانات مع مراعاة الشروط المنصوص عليها في المعاهدات الدولية".[3]

الفرع الثاني : تفتيـــش النظـــام بـــدون إذن:

القاعدة العامة أن تفتيش النظام أو الجهاز لا يجوز إلا بعد الحصول على إذن للقيام بهذا الإجراء من قبل الجهة المختصة، و هذه القاعدة يمكن أن ترد عليها استثناءات فيها حالة التلبس.

فلا يجوز تفتيش الكمبيوتر دون الحصول المسبق على إذن بذلك، استنادا إلى كون التفتيش يأخذ حكم تفتيش الشخص و هذا ما استقر عليه العمل في كثير من التشريعات [4] تأكيدا على كون أن للفرد حرمة لحياته الخاصة بحيث لا يجوز الاعتداء عليها باتخاذ إجراء يخالف التوقع المعقول للحياة الخاصة.[5]

و لم يؤكد هذا الحق فقط المشرع بل نحى نحوه القضاء، فقد فسرت المحاكم الأمريكية معيار الحماية الدستورية لهذا الحق بأن إجراء التفتيش يقع مخالفا للدستور [6] متى خالف معيار "التوقع المعقول للحق في الخصوصية" سيما و أن البعض يعتبر الكمبيوتر من قبيل الصندوق المغلق أثناء إجراءات التحري و التحقيق و هذا المنطلق انحاز له القضاء الأمريكي في كثير من

---

[1] - النص بالفرنسية عند شيماء عبد الغني ، مرجع سابق ، ص عبد الغني، ص 203.

[2] - شيماء عبد الغني ، مرجع سابق ، ص عبد الغني، ص 302.

[3] - النص بالفرنسية عند شيماء عبد الغني ، مرجع سابق ، ص عبد الغني، ص 302.

[4] - نص الدستور الأمريكي في التعديل الرابع منه على "حق الأفراد في حرمتهم الشخصية و حرمة منازلهم و أوراقهم و أموالهم المنقولة في مواجهة التفتيش غير المعقول و الضبط يتعين احترامه و لا يجوز أن يصدر إذن التفتيش إلا بناء على تحريات جدية و يحدد في هذا الإذن بمكان محل التفتيش و الأشخاص و كذلك الأشياء المطلوب ضبطها"، النص بالانجليزية عند شيماء عبد الغني ، مرجع سابق ، ص عبد الغني، ص 309.

[5] - شيماء عبد الغني ، مرجع سابق ، ص عبد الغني، ص 309- 310.

[6] - اجتهدت المحاكم الأمريكية إلى قياس الأجهزة المخزنة الكترونيا على الصناديق المغلقة فاستندت في ذلك على كون الدخول للمعلومات المخزنة داخل الجهاز متماثل مع فعل فتح الصناديق المغلقة التي تكسب الأفراد حق التوقيع المعقول للحياة الخاصة على محتوياتها، شيماء عبد الغني ، مرجع سابق ، ص عبد الغني، ص313.

أحكامه[1] حيث اعتبر المعلومات التي يحويها الجهاز من قبيل الأموال المنقولة لحائز الجهاز و يقبل منه أن يتمسك بالتوقع المعقول للحياة الخاصة.[2]

01- حـــالات تفتيـــش جهـــاز الحاســـب بـــدون إذن "الاستثناءات":

أبرز التشريعات التي حددت الاستثناءات الواردة على التفتيش بإذن (أي متى يقع التفتيش بدون إذن صحيحا هو المشرع الأمريكي و أبرز هذه الاستثناءات هي:[3]

التفتيش الذي لا يخالف التوقع المعقول للحياة الخاصة.

حالة الرضاء

التفتيش على إثر الضبط الصحيح

حالة الضرورة

حالة التلبس عند وجود الجهاز خارج المنزل

حالة جرد الأشياء المضبوطة

تفتيش الجمارك

تفتيش شبكة الإنترنيت

أ/ حـــق التوقـــع المعقـــول للحيـــاة الخـــاصة:

ألا يخالف التفتيش التوقع المعقول للحياة الخاصة:

لم يرد في الدستور الأمريكي تعريف لحق التوقع المعقول للحياة الخاصة إلا ما ورد من عبارات من نصوص في التعديل الرابع باستخدامه ذات الألفاظ "الفرد له حق في أن يأمن على نفسه و بيته و أمواله المنقولة و مستنداته ضد أي ضبط أو تفتيش غير معقول، حيث يجب عدم مخالفة هذه الحقوق، غير أن التفتيش إذا استند إلى سبب معقول و بناء على تحريات جدية فإنه تقع صحيحا"[4]

غير أن غياب المعيار الذي يمكن أن يعتد به في الفصل في النزاعات و حماية الحقوق و إقرار الأحكام – بإغفال من المشرع – اجتهد القضاء الأمريكي في إيجاده حيث اجتهدت المحكمة

---

[1] - يمنع بوجه عام على رجال الضبط القضائي الدستور الأمريكي من فتح أو الاطلاع على المعلومات المخزنة في الجهاز بدون إذن قياسا على منع الدخول و فتح الصناديق المغلقة و فحص محتوياتها، شيماء عبد الغني ، مرجع سابق ، ص عبد الغني، ص 313.
و تجدر الإشارة إلى أن الدستور الأمريكي يخلو من تعريف لماهية التوقع المعقول للحياة الخاصة، شيماء عبد الغني ، مرجع سابق ، ص عبد الغني، ص 312.

[2] - شيماء عبد الغني ، مرجع سابق ، ص عبد الغني، ص 310.

[3] - شيماء عبد الغني ، مرجع سابق ، ص عبد الغني، ص 311.

[4] - شيماء عبد الغني ، مرجع سابق ، ص عبد الغني، ص 311. أنظر أيضا:

Bruno P. LANGLOIS, La protection des marques sur internet : le législateur fédéral américain s'attaque à la cyber piraterie, Revue Gazette du Palais, 20 juillet 2000 n° 202, P. 29Cyril

العليا الأمريكية في إصدار بيان متى يكون الشخص العادي له الحق في التوقع المعقول للحياة الخاصة فقد قضت بأن الشخص له الحق في التوقع المعقول للحياة الخاصة على الأموال المتواجدة داخل منزله، كما اعتبرت هذا المعيار متوافر أيضا بالنسبة لمحتويات الصناديق المهتمة التي لا يتبين ما بداخلها، و التي يمكن تفتيشها إلا بعد الحصول على إذن فالتفتيش من الجهة المختصة، و هذا المعيار ينسحب على الحاسب لتماثل الأخير مع الصناديق المعتمة في وضعها القانوني لإجراء التفتيش.[1]

أثير التساؤل عن مدى توافر الحق في التوقع المعقول للحياة الخاصة بالنسبة لجهاز الحاسب أو بالأدق المعلومات أو البيانات المخزنة فيه[2] و استقر على أنه لا يمكن الدخول إلى هذه البيانات إلا بعد الحصول على إذن متطابق وصف الجهاز مع الصندوق المقفول و أيد الدستور الأمريكي هذا الاتجاه بأن منع رجال الضبط القضائي بشكل عام الدخول و رؤية البيانات أو المعلومات المخزنة في الجهاز بدون إذن قياسا على منع الدخول و فتح الصناديق المغلقة و فحص محتوياتها.[3]

ب/ الرضـــاء بالتفتيـــش:

إذا كان صاحب الجهاز أو حائزه موافقا على تفتيشه فإن هذا الرضاء لاغ لإذن التفتيش حيث لا يلزم صدور إذن بإجراء التفتيش طالما صاحب الجهاز برضائه رفع القيد الوارد على إجراء التفتيش.

نشير إلى أن التفتيش يمتد أثره إلى الحدود التي يضعها صاحب الجهاز أي أن هذه الموافقة إذا صدرت صحيحة من صاحب الحق في الجهاز فإنها تصبح (الموافقة) محددة للنطاق الذي يصح في إطاره التفتيش، و يقضى ببطلان الإجراء و استبعاد أدلته إذا تجاوز نطاق الرضاء المصحح للتفتيش غير أن التشريع الأمريكي توسع توسعا يكاد يخل بحقوق الأفراد في مسألة توسيع صاحب الحق في الرضاء و اعتبار كل من يمكنه استعمال الجهاز له الحق أنه يسقط إذن التفتيش برضائه [4] و من جهة أخرى يقع التفتيش بالوصف الذي سبق مع اعتراض صاحب الجهاز الحاضر.

---

[1] - شيماء عبد الغني ، مرجع سابق ، ص عبد الغني، ص 312- 313.

[2] - شيماء عبد الغني ، مرجع سابق ، ص عبد الغني، ص 313.

[3] للإطلاع أكثر على أثر إجراء التفتيش على حق التوقع المعقول للحياة الخاصة أنظر شيماء عبد الغني ، مرجع سابق ، ص عبد الغني، ص 311-316.

[4] - شيماء عبد الغني ، مرجع سابق ، ص عبد الغني،ص ص318 327.

لكن يهمنا ما له علاقة وثيقة بالتحقيق في جرائم التجارة الالكترونية حيث النظام هو المرتكز للمبادلات الالكترونية فيثار التساؤل حول سلطة مديري النظام – أي أو لا ... المشرفين على شبكة الإنترنيت من ناحية التشغيل و الصيانة – في الرضاء بالتفتيش، و هذه المسألة أعقد من سابقتها فالإشكال مطروح حول سلطته في الرضاء بتفتيش الشبكة أي الاتصالات التي تتم بين أجهزة الحواسيب التي هو مسئول عنها فوفقا للقواعد العامة ليس له أن يرضى بتفتيش من يشرف هو عليهم[1] قياسا على كون أن صاحب المحل التجاري ليس من حقه أن يرضى بتفتيش ..... تركها عنده أحد رواد المحل عند دخوله إليه، غير أن المشرع الأمريكي سمح بذلك بمقتضى نصوص تضمنها قانون الاتصالات الالكترونية و الحق في الخصوصية[2].

أما عن مدى كفاية الرضاء الصادر من مدير الشبكة التي تتصل أجهزة المستخدمين الذين لم يصدر بخصوصهم إذن بالتفتيش، فإن هذا الأمر مرهون بالعلاقة القائمة بين القائم بالتسكين و بين أصحاب المواقع فإذا ما سبق الاتفاق على أن يراقب القائم بالتسكين رسائل أصحاب المواقع و أن يتعاون مع السلطات القضائية جاز بذلك التفتيش برضاء بدون إذن و كذا الحال محال بالنسبة لرب العمل فله الحق في أن يراقب أجهزة مستخدميه للتأكد من عدم إساءة أو استعمال أجهزة الشركة في غير الغرض المخصص له كما له أن يوافق على التفتيش.[3]
و يرى البعض[4] أن المشرف على النظام له أن يقوم بمراقبة النظام بالقدر اللازم لتشغيله دون أن يتعسف في هذا الحق فيمتد إلى نسخ الملفات أو تسجيل البريد الالكتروني مثلا.
مسألة أخرى اعتد بها كذلك المشرع الأمريكي و هي الرضاء الضمني تحذيرا للمستخدم من أنه إذا استمر في استغلال الشبكة فإن إمكانية مراقبته قائمة، فإذا دخل و استخدم الشبكة فإن ذلك يعد رضاء ضمنيا منه بالمراقبة.

ج / حالـــة الضـــرورة:

أقرت بعض التشريعات الضرورة كمسوغ لتفتيش الأشخاص دون وجود إذن بذلك و لعلها تجد مسوغا أكبر في مجال جرائم التجارة الالكترونية بسبب سهولة إتلاف الدليل على الجريمة أو

---

[1] - شيماء عبد الغني ، مرجع سابق ، ص عبد الغني، ص ص 319 329.

[2] **Bruno P. LANGLOIS, La protection des marques sur internet : le législateur fédéral américain s'attaque à la cyber piraterie, Revue Gazette du Palais, 20 juillet 2000 n° 202, P. 29Cyril**

[3] - شيماء عبد الغني ، مرجع سابق ، ص عبد الغني، ص 330- 331.
[4] - شيماء عبد الغني ، مرجع سابق ، ص عبد الغني، ص 331.

ضياعه إذا كان دليلا الكترونيا و طبق القضاء الأمريكي هذه الفكرة عندما قضى بأن رجل الضبط لا يحتاج إلى إذن بتفتيش جهاز الكمبيوتر إذا شاهد المتهم و هو ما يقوم بمحو ملفات سجله تتعلق بالجريمة المتحري عنها في هذا الجهاز أو إذا ما قام من الظروف ما يسمح بالاعتقاد بشكل معقول بأن المتهم سوف يقوم بمحو أدلة تفيد في كشف الحقيقة عن الجريمة، كما قضت المحاكم الأمريكية بصحة مخزنة في جهاز كمبيوتر متواجد في الخارج طالما حدث به إتلاف أو فقدان البيانات – الدليل على ارتكاب الجريمة – لها من الأسباب المعقولة ما يبررها و ما تثيره هذه الحالة من إشكالات هو تقدير حالة الضرورة.[1]

د/ حالـــة التلبـــس:

عموما يصعب إهمال قواعد التلبس في مجال جرائم ذات الطبيعة الالكترونية و فيها جرائم التجارة لأنها تتميز بالحفاء الشديد و لا يظهر فيها الركن المادي للعيان كما في الجرائم التقليدية كونها جريمة تقنية منطقية سلوكيات الركن المادي تتم في العالم الافتراضي الذي يصعب على رجال الضبط إدراكها في حالة تلبس، و من صور هذه الحالة ما انتهجته بعض التشريعات مؤخرا – و بعد تنامي بعض الظواهر الإجرامية ذات الأثر الماد ي التي يعتمد على تقنيات التجارة الالكترونية و لكنها ذات محل غير مشروع كالمخدرات و تجارة الجنس – أصبحت تعاقب على مجرد حيازة بيانات متعلقة بمثل هذه التجارة. و كيفت وجود بيانات هذا الاتجار بحالة التلبس.[2]

هـــ /حالـــة القبـــض الصحيـــح:

القاعدة العامة تقضي بأنه كلما جاز القبض و ذلك بالنسبة للفرد و المنطقة المحيطة به جاز التفتيش، و اعمالا لهذه القاعدة فإن أحكام القضاء الأمريكي اتجهت إلى إقرار صحة تفتيش الأجهزة الالكترونية التي تتواجد بصحته المتهم الذي قبض عليه على وجه صحيح.[3]

فرقت أحكام القضاء فيها القانون الأمريكي و يبين أماكن العمل الخاصة و أماكن العمل بالنسبة للموظف صاحب الجهاز فالنسبة إلى أماكن العمل الخاصة يتمتع الموظف بالحق في الخصوصية لأماكن عمله و لا يجوز لرجل الضبط التفتيش بدون إذن إلا بموافقة رب العمل أو للمدير في العمل أو من مستخدم له سلطة على تلك الأماكن الخاص لأن رضائهم بالتفتيش يعتد به بالنسبة لأماكن العمل الخاصة، كما ذهبت أحكام القضاء الأمريكي أبعد من ذلك عندما أجازت رضاء المستخدم بتفتيش ممتلكات خاصة برب العمل لأنها تتواجد في أماكن للعمل قد

---

[1] - شيماء عبد الغني ، مرجع سابق ، ص عبد الغني، ص 334- 336.

[2] - أنظر المادة 178 عقوبات مصري لقانون 95 لسنة 1996، شيماء عبد الغني ، مرجع سابق ، ص عبد الغني، ص 339.

[3] - شيماء عبد الغني ، مرجع سابق ، ص عبد الغني، ص 341.

سمح له بالاستعمال الكامل لها فقد يكون الموظف مندوب مبيعات أو قائم على الإعلانات أو مكلف بالإيداع و تحويل المبالغ المدفوعة أما بالنسبة لأماكن العمل العامة فإن أحكام القضاء الأمريكي و أحكام القضاء في التشريعات المقارنة فإنها و استثناءا من الأصل العام _ أي حق الفرد في الخصوصية _ تتجه إلى الاعتداد بالرضاء بالتفتيش إذا كان هذا الرضاء مبادرا من الرئيس الإداري، كما اعتبرت هذه الأحكام القضائية برضاء الزملاء العامليين في نفس المكتب بتفتيش المكتب المشترك.[1]

كما إعمال مبدأ جرد المضبوطات و تحريرها على الوجه الصحيح يثير إشكالات عديدة في مجال المضبوطات الالكترونية لوجود مبرر لفتح توابع الجهاز المخزنة للبيانات و الاطلاع عليها (كالأقراص و U.S.B)[2].

الفرع الثالث : حالـــــة تفتيــش الشبكـــــة:

لا معنى للمبادلات التجارة الالكترونية دون شبكة الإنترنيت و لولا هذه الشبكة ذاتها لما طور الجرمون أساليب سلوكاتهم الإجرامية و لكونها شبكة مفتوحة يجوز إليها و الإطلاع و ضبط البيانات المتاحة للجمهور بدون إذن تفتيش، لكن قد يصعب تعقب الجناة المحترفين في جرائم التجارة الالكترونية دون تعاون مزودي الخدمات الوسيطية[3] المتواجدين داخل الإقليم و لا يطرح ذلك أي مشكل فقد علمنا سلفا أنهيجب عليهم التعاون مع الجهات القضائية كما أقرته بعض التشريعات، لكن بالنسبة لمزودي الخدمات خارج الإقليم كون أن جريمة التجارة الالكترونية هي من الجرائم الممتدة خارج حدود الدولة نظرا للطبيعة التي تتميز بها المبادلات و قد قضى بصحة تفتيش الأجهزة الالكترونية التي تتواجد بصحبة المتهم الذي تم القبض عليه على الوجه الصحيح.[4]

لكن هل يمكن تفتيش أجهزة يستخدمها الموظف في شركة مثلا مبادلاتها التجارية الالكترونية دون أن يكون مالك لتلك الأجهزة أو الحواسيب؟ حول هذا الإشكال نجد أن أحكام القضاء في التشريعات المقارنة فرقت التجارة الالكترونية فإن تعاون هؤلاء الوسطاء متوقف على إجراء طلب المساعدة القضائية لتعلق هذا الإجراء بسيادة الدولة التي يتواجد بها مزود الخدمات فقط و ليس من قبيل أن التفتيش مواقع هذه التجارة تسري عليها أحكام و قواعد تفتيش المساكن و لا تقر لها التشريعات المختلفة ذات الحماية المقررة للمسكن الخاص.

---

[1] - شيماء عبد الغني ، مرجع سابق ، ص عبد الغني، ص 342- 344.
[2] - راجع شيماء عبد الغني ، مرجع سابق ، ص عبد الغني، ص 349.
[3] - إرجع إلى الباب الأول.
[4] - شيماء عبد الغني ، مرجع سابق ، ص 341.

فأطراف العلاقة التعاقدية الالكترونية حينما ينتشرون بياناتهم على الشبكة هم على علم أن هذه العلاقة عملية تقنية تتم بواسطة وسيط مزود خدمات الذي لا يستلزم للاطلاع هذه البيانات لديه سبق الحصول على إذن بالتفتيش فشبكة نظام مفتوح و ليس لها حرمة المسكن الخاص.[1]

إلا أن التفتيش ليس في هذا المجال بالحق المطلق بل ترد عليه بعض الاستثناءات تشكل حدودا ترد عليه منها ما تعلق بـــ:

01- حمايـــة البيانـــات المتعلقـــة بالحـــق فـــي الخصوصيـــة:

و قيد كثير من التشريعات بوضعها لقواعد خاصة لتفتيش الأجهزة أو المواقع التي تحوي هذه البيانات المتعلقة بالحالة الاجتماعية و الحالة الصحية و الحالة الوظيفية و الحالة الجنائية و قد سبق أن تطرقنا لذلك.[2]

02- حمايـــة بيانـــات الأفـــراد لـــدى الجهـــات القضائيـــة:

تنظم بعض التشريعات سلطة من له حق الاطلاع أو الدخول إلى الأنظمة التي تحوزها جهات قضائية (النيابة العامة، المحاكم، جهات الضبط القضائي) إلا بمقتضى أمر قضائي أو بإجازة صريحة كالحالات التي تجيز لرجال الضرائب الاطلاع على تلك البيانات و بهدف مكافحة التهرب الضريبي [3] و يقيد بتفتيش هذه البيانات بالقيود التي نصت عليها القوانين كالمعلومات المتعلقة بسر المهنة و المعلومات المتعلقة بأسرار الدولة الاقتصادية و على سبيل المثال أعفى القانون الهولندي بالنص صراحة على إعفاء أصحاب المهن الذين يعفون أصلا من الشهادة من أن يخضعوا الإجراءات التفتيش إلا إذا أجاز أصحاب الأسرار ذواتهم إجراء التفتيش، و مثلها بيانات الموكلين لدى المدافعين عنهم (المحامين) حيث وضعت لتفتيشها نظام خاص[4] و قد تتخذ هذه البيانات طابعا الكترونيا و كذلك العلاقة أيضا بين الموكل و محاميه.

المطلب الثالث : قواعـــد الضبـــط فـــي مجـــال التعامـــلات الالكترونيـــة:

مجـــال الضبـــط:

بالنسبة لإجراءات الضبط توفر العناصر المستقلة الالكترونية التي يمكن أن يطالها الضبط بسهولة في التعامل من قبل الجهات القضائية إذا ما تعلقت هذه العناصر بجريمة وقعت متحري

---

[1] - شيماء عبد الغني ، مرجع سابق ، ص عبد الغني، ص 351.

[2] - تنص المادة 125 من القانون الهولندي على "أن يتم محو البيانات التي تنتمي إلى هذا النوع و يقوم بهذا المحو الشخص الذي سبق أن قام بتسجيل هذه البيانات "، النص بالفرنسية عند شيماء عبد الغني ، مرجع سابق ، ص عبد الغني، ص 353- 354.

[3] - **Michel AUJEAN, L'évolution de la fiscalité en Europe sous l'impulsion de la Commission : 50 ans du Traité de Rome, Revue Gazette du Palais, Communautés européennes, 10 juillet 2007 n° 191, P. 16**

[4] - شيماء عبد الغني ، مرجع سابق ، ص عبد الغني، ص 356.

عنها، لكن حينما يتعلق الضبط بالجرائم الالكترونية و بالأدق حينما يتعلق الضبط بالجرائم الالكترونية و بالأدق حينما يرد على أشياء ذلت طبيعة معنوية (البيانات) فإن هذا الإجراء يختلف عنه في ضبط أداة الجريمة في الجرائم التقليدية و رغم ذلك لم يرد بشأنه نص خاص في قوانين الإجراءات الجنائية ضد مختلف المشرعين مما يجعل تطبيق و سريان القواعد العامة على ضبط المعلومات مادامت تشكل موضوع الجريمة التي وقعت أو الأداة التي استخدمت في ارتكابها أو هي من متحصلات الجريمة أو هي تفيد في إثبات الحقيقة بشكل عام.[1]

و هذا ما سمحت به بعض التشريعات.[2]

إذا لم يؤدي إلى تعطيل كل العمل في النظام و الشبكات المتصل بها كما يتعين المحافظة على سرية البيانات التي تم ضبطها و التي يحمي القانون طابعها السري و تحفظ بالطريقة التي تضمن سلامة الدليل الالكتروني و صحته بغرض تقديمه لسطلة التحقيق أو لتدعيم التعاون الدولي.

في هذا المجال كما جاء في التوصية رقم 13 لسنة 1995 كما أوصت بتطبيق القواعد المتعلقة بالمستندات التقليدية على المعلومات المخزنة الكترونيا في الكمبيوتر أو النظام.[3]

كما أجازت الاتفاقية الأوربية لجرائم السيبر لعام 2001 أن يتم الضبط عن طريق أخذ نسخة من تلك البيانات فيما تضمنته المادة 19 من القسم الرابع بأنه " من سلطة كل دولة طرق أن تتخذ الإجراءات التالية:

أن تضبط نظام الكمبيوتر أو جزء منه أو المعلومات المخزنة على وسيط من وسائط التخزين الخاصة بالكمبيوتر و أن تحتفظ على سلامة تلك المعلومات المخزنة".[4]

---

[1] - شيماء عبد الغني ، مرجع سابق ، ص عبد الغني، ص 357.

[2] - تسمح م 41 من قانون الاجراءات الجنائية الفيدرالية الأمريكي و بعض نصوص قانون الإثبات في المملكة المتحدة البريطانية، شيماء عبد الغني ، مرجع سابق ، ص عبد الغني، ص 357.

[3] - النص الأصلي عند شيماء عبد الغني ، مرجع سابق ، ص عبد الغني (3)، ص 359.

[4] - النص الأصلي عند شيماء عبد الغني ، مرجع سابق ، ص عبد الغني، ص 361.

المبحث الثالث : حجية المخرجات الالكترونية امام القاضي الجنائي

دليل الإثبات في الجرائم التقليدية مرئي أو مادي كيفما كانت الكيفية التي ارتكبت بها الجريمة مما يسهل على رجل الضبطية أو رجال التحقيق الجنائي رؤية الدليل و ملامسته بالحواس، لكل هذا بذات البساطة أو بذات السهولة بالنسبة للجريمة (المعلوماتية) لجرائم التجارة الالكترونية. فالبيانات أو المعلومة في الجرائم عبارة عن نبضات الكترونية غير مرئية تنساب عبر شبكة الانترنيت و ما يتصل بها من أنظمة معالجتها الأولى آليا و عادة ما تكون مشفرة لا يفك رموزها إلا النظام الآلي أو الجهاز الالكتروني.[1]

و قد أسفرت هذه التقنية عن تقلص تدريجي لدور المخرجات الورقية كوعاء تقليدي للمعلومات و الأدلة بالتالي، و ازدياد مطرد تقابلي في كم المعلومات المنتجة أو المعروضة في أو غير لا ورقية مستحدثة أو هي بالتالي كذلك أدلة غير مادية في مجال الإثبات الجنائي ما يفرض على أجهزة العدالة و القضاء تطوير أساليب كشف هذه الجرائم، و الوسائل المستخدمة في و تحديث المنظومة القضائية للتعامل مع هذه الجرائم الوصول إلى الحقيقة، و ضرورة تحديث الأساليب الإجرائية و استكمالها على النحو الذي يكفل استجابتها لمتطلبات العملية الاثباتية في مجال المعاملات التجارة الالكترونية[2] هذا من جهة و من جهة أخرى فإن هذا النمط من الأدلة غير المحسوسة أثار العديد من المشاكل العملية في مجال الإجراءات الجنائية أبرزها:[3]

مشكلات متعلقة بمدى كفاية أساليب..... التقليدي في التقنين الإجرائي لإجراء التحقيق و جمع الأدلة في بيئة الكترونية.

مشكلات إجرائية مستحدثة تبعا لطبيعة التعاملات التجارية الالكترونية من قبيلها حساب مدة التقادم، إلزام الشاهد على كشف كلمات السر، تسجيل البيانات و الاطلاع عليها و مدى جواز ذلك.

مشكلات طرحت بخصوص مسألة التعاون الدولي لمكافحة هذه الجرائم فيما تعلق (بدائرة الاختصاص) نطاق الاختصاص وجهة التحقيق و الإدعاء و المحاكمة.

فمخرجات الالكترونية ليس دائما ورقية بل إن البيانات المخزنة أو المسجلة هي أضعاف تلك التي خرجت على دعامات مادية (ورقية) و هذه البيانات – التي لديها القابلية للشكل

---

[1] - حجازي، الدليل، ص 36.
[2] - فريد رستم، المؤتمر، ص 418-419.
[3] - فريد رستم، الجوانب الإجرائية، ص 06.

كمخرجات الكترونية – يثار حولها التساؤل حول مدى القوة الثبوتية لها [1] و إلى أي مدى يمكن قبول المخرجات الالكترونية و ما مدى حجيتها الاثباتية ؟[2]

أو ما مدى إمكانية مسايرة رسائل الإثبات الجنائي التقليدية مع تقنية المعاملات التجارية الالكترونية ؟

و لو أصح من هذه التساؤلات أنها ترشد إلى ظهور مفاهيم جديدة أو حديثة على مستوى القانون الجنائي..... اعتماد المعاملات التجارية على التقنية الرقمية ذات الطبيعة التقنية المنبثقة عن الحاسوب و الانترنيت حيث أفرز هذا الارتباط بين المظاهرة الرقمية كآلية حديثة للتعاملات التجارية و بين الإثبات الجنائي على مفهوم الدليل الرقمي أو الدليل الالكتروني، و قد اعتدت به المحاكم في النظم القانونية المقارنة و أعطته الحجية القانونية ذاتها التي يملكها الدليل الجاري أو التقليدي المستمد من إجراءات الحصول عليه كالتلبس، التفتيش، الشهادة و القرائن و الاعتراف.[3]

شـــروط قبـــول الدليـــل المعلوماتـــي:

المطلب الأول : المخرجـــات الالكترونية في نظم الإثبات عند التشريعات المقارنة:

ينبغي الإشارة أولا إلى ذلك التقسيم الذي أورده فقهاء القانون المقارن حول تصنيف الشرائع و كذلك تصنيف نظم الإثبات،

و لعل تصنيف أكثر الشرائع على أساس الاختلاف في الصياغة القانونية إذ اعتمد على على توزيعها على ثلاث أقسام:[4]

قوانين ذات صياغة لاتينية: مصادر القانون فيها واحدة و أصولها العام متحدة و تقسيماتها متماسكة و الاصطلاحات القانونية فيها متشابهة كذلك الأسلوب و الصياغة متقاربان.

قوانين أنجلو سكسونية: أو ما يعرف بقانون العام الانجليزي *Commun Law* قانون مستقل بذاته من حيث المصادر و الاصطلاحات القانونية و الصياغة.

قوانين ذات صياغة مختلطة

– أما عن نظم الإثبات فهي كذلك ثلاث أصناف و أساس ارتكازها على فكرتان:[5]

نظام الإثبات القانوني أو المقيد

نظام الإثبات المعنوي أو المطلق

---

[1] - يتعلق الإثبات في المواد الجنائية بأركان الجريمة أي بالركن المادي و الركن المعنوي و هو بعينه يختلف عن الإثبات في المواد المدنية الذي يتعلق بالالتزامات التي تربط الأطراف، شيماء عبد الغني ، مرجع سابق ، ص عبد الغني، ص 386.

[2] - هلالي عبده ، مرجع سابق ، ص، حجية المخرجات، ص 13.

[3] - عمر بن يونس، ص 966.

[4] - هلالي عبده ، مرجع سابق ، ص، حجية المخرجات، ص 25- 27.

[5] - عبده هلالي، حجية، ص 27.

نظام الإثبات المختلط

و الأساس الذي تقدم عليه هذه الأنظمة هو فكرتان:

تحديد أو عدم تحديد أدلة الإثبات المعروضة على القضاء

تقرير أو عدم تقرير القيمة الإقناعية لكل دليل

فإذا ما حدد المشرع أدلة الإثبات و قدر قيمتها الإقناعية كنا أمام نطاق الإثبات المقيد أو الأدلة القانونية و هذا النظام سائد ليحكم القوانين ذات الصياغة أنجلو سكسونية.

أما إذا ترك المشرع تحديد الأدلة و تقدير قيمتها الإقناعية و أوكل ذلك للقاضي كنا أمام نظام الإثبات الحر أو الأدلة المعنوية، و هذا النظام يعتمد فيه القوانين ذات الصياغة اللاتينية.

و أما إذا ما حدد المشرع أدلة الإثبات و فسح للقاضي سلطة تقدير قيمتها الإقناعية كنا أمام نظام مختلط و هذا النظام سائد في القوانين ذات الصياغة المختلطة.

لم تورد التشريعات الحديثة نصوصا تضبط شروط تقديم الدليل المعلوماتي و طريقة تقديره من قبل المحكمة عدا بعض القواعد التي تضمنتها بعض التشريعات كالنمسا، اليونان، سويسرا و النرويج حيث تطلبت في الأدلة الالكترونية أن تكون مقروءة (على شاشة الجهاز أو على ورق)[1] و هذا لا يثير حجية الأدلة الالكترونية إشكالا بالنسبة للدول ذات الصياغة اللاتينية حيث يسود مبدأ حرية الإثبات و الاقتناع و بالنسبة للمواد الجنائية فإن السائد هو مبدأ حرية القاضي الجنائي في تكوين عقيدته لعدم تقيده بدليل معين و عليه فإن المخرجات الالكترونية تصلح لأن يأخذ القاضي بها في تكوين عقيدته و استيفاء اقتناعه إذا ما اطمأن يقينه لصحة تلك المخرجات أو المحررات[2]، فإن الأساس هو حرية القاضي في تقدير هذه الأدلة.[3]

الفرع الاول : التشريعات اللاتينية :

ففي فرنسا يدرس الفقه مسألة حجية المخرجات الالكترونية في المواد الجنائية ضمن مسألة أوسع و أعم هي مسألة قبول الأدلة الناشئة عن الآلة أو الأدلة العلمية [4] هذه الأدلة أخذ بها المشرع و قبلها القضاء بشروط أهمها أن يتم الحصول على الدليل بطريق شرعي و..... و كذلك أن يتم مناقشتها حضوريا عن طريق الأطراف.[5]

---

[1] - شيماء عبد الغني ، مرجع سابق ، ص، ص 386.

[2] - شيماء عبد الغني ، مرجع سابق ، ص، ص 385.

[3] - هلالي عبده ، مرجع سابق ، ص، المؤتمر 721، 222.

[4] - هلالي، المؤتمر، 722.

[5] - هلالي، حجية، 43.

أما في تونس فقد اشترط في الأدلة الالكترونية أو مخرجات الحاسب الآلي أن يتم الحصول عليها بطريق مشروع و على نحو نزيه، عندما أثير التساؤل عن مدى قبول الأدلة الناشئة عن الآلة في مجال الإثبات.

أما في لوكسمبورغ فإن القانون لم يقم في المجال الجنائي نموذجا خاصا للإثبات و بحكم أن مبدأ الاقتناع الذاتي للقاضي هو المعتمد في الأحكام الجنائية فإن المخرجات الالكترونية لم تتأثر بها الأحكام القضائية و لا طرق الإثبات المعتمدة حيث لقاضي الموضوع حرية التقدير و له السيادة على القيمة الدافعة للعناصر الاثباتية التي يؤسس عليها اقتناعه و يكون للأطراف حرية الاعتراض عليها في كافة مراحل الدعوى.

و يصح في تركيا أن تقدم كدليل أمام القضاء تسجيل البيانات التي يتم نقلها بواسطة نظم الاتصال في إطار إثبات جرائم مرتكبة عن طريق المعلوماتية.[1]

التشريعات الانجلو سكسونية :

أما في الولايات المتحدة الأمريكية فإن النصوص الواردة في قانون الإجراءات الفدرالي اتجهت إلى الاعتداد بالأدلة الالكترونية فالقاعدة 3/1001 أكدت على قبول الدليل الالكتروني باعتباره مستندا أصليا مادام أن البيانات الصادرة من الكمبيوتر مقروءة للعين المجردة و معبرة عن البيانات الأصلية بشكل دقيق و لا تختلف حجيتها من حيث كونها مطبوعة أو مسجلة على دعامات أخرى، و هذه القاعدة سبقتها الفقرة الأولى من م 1001 التي عرفت الكتابة و التسجيلات بأنها حروف أو أرقام أو كلمات أو ما يعادلها مكتوبة على اليد أو منسوخة على الآلة الكاتبة أو مطبوعة أو تم تصويرها أو اتخذت شكل نبضات مغنطيسية بتسجيل ميكانيكي أو الكتروني أو أي شكل آخر من تجميع المعلومات.[2]

و تنص المادة 6/803 من القواعد الإجرائية الأمريكية على قبول الدليل الالكتروني المستمد من مذكرة أو تقرير أو بتسجيلات تم الاحتفاظ بها أثناء القيام بنشاط تجاري منتظم.[3]

و النصوص التي تناولت حجية الأدلة الالكترونية عديدة في القوانين الأمريكية التي أكدت على قبول المخرجات الالكترونية كأدلة إثبات.[4]

---

[1] - هلالي، المؤتمر، 722 / هلالي، الحجية، ص 44.

[2] - شيماء عبد الغني ، مرجع سابق ، ص، ص 388.

[3] - شيماء عبد الغني ، مرجع سابق ، ص، ص 389.

[4] - قانون الحاسب الآلي لسنة 1984 الصادر في ولاية Ioma، و قانون الإثبات الصادر في 1983 في ولاية كاليفورنيا / الهلالي، الحجية، ص54/ هلالي، المؤتمر، 729.

وانتهج القضاء الأمريكي ذات النهج في أحكامه من كون أن المخرجات الالكترونية (هي) تكون مقبولة طالما أن الجهاز الآلي المستخرجة منه يعمل بشكل سليم و المشرف و توفرت الثقة و الطمأنينة في القائم عليه.[1]

أما في بريطانيا فقد اشترط المشرع شروطا معينة لقبول المستندات الالكترونية في بعض الحالات بنص صريح و ذلك منذ وقت بعيد [2] في مجال المعاملات التجارية و أهم هذه الشروط هي:[3]

فقانون الشرطة و الإثبات الجنائي الذي صدر سنة 1986..... في مادته 69 على ذلك و أهم الشروط التي في المادة 1001/ 1 من قانون الإثبات الأمريكي تم تطويرها لتشمل الدليل الرقمي على أوسع نطاق حيث سمحت بالاعتراف بالمواد المكتوبة و المسجلة و الالكترونية.[4]

اشترطها:

سلامة الجهاز المستخرج منه الدليل.

سامة الدليل ذاته من عيب الاستخدام غير المناسب أو الاستخدام الخاطئ للجهاز.[5]

الوفاء بأي شرط تحدده قواعد المحاكمة.

المطلب الثاني : إشكالات الدليل الالكتروني في الإثبات في المواد المدنية أمام القاضي الجنائي

الإشكال في السماح باعتماد الدليل الالكتروني في الإثبات في المواد المدنية يكمن في كون مقدمة..... في الخصومة و عدم الثقة فيه لسهولة تعديل البيانات التي يحتويها أو إعداده أصلا بالأخص أن العلاقة التعاقدية التجارية تفتقر إلى التوازن فالطرف القوى المحترف طرف قوي إذا ما قورن بالمستهلك الذي هو في مركز أضعف و..... من عوامل قوة الطرف الأول تمكنه من تكنولوجيا المعلومات و بذلك حكم بضعف القوة الثبوتية للمحرر أو الدليل إذ كان صادرا من أجهزة أحد الخصوم و لا يعول على شهادة خصم في الدعوى في المواد المدنية إلا أن البعض قد خالف هذا الاتجاه بالقانون المدني في مقاطعة..... سمح في بعض مواده بالاستناد إلى البيانات الصادرة من التاجر لاعتمادها كدليل في الإثبات إذا توفرت الشروط الآتية:[6]

وضوح البيانات

---

[1] - هلالي، الحجية، ص 54- 55.

[2] - صدر سنة 1965 قانون بشأن السجلات التجارية سمحت فيه بنصوص صريحة قبول الدليل الالكتروني، شيماء عبد الغني ، مرجع سابق ، ص، ص 389.

[3] - شيماء عبد الغني ، مرجع سابق ، ص، ص 389- 390.

[4] - للاستفاضة أكثر أنظر عمر بن يونس، ص 986- 994.

[5] - سلامة المخرجات الالكترونية ترتكز على سلامة و صحة برنامج التشغيل الذي يتحكم في عمل الجهاز.

[6] - شيماء عبد الغني ، مرجع سابق ، ص، ص 400.

ضمانة الثقة في الجهاز بما يقره من ضمانات

تحدد المحكمة ضمانات الثقة

تفترض المحكمة وجود ضمانات الثقة في النظام بشرطين:

دخول بيانات المعادلة التجارية في جهاز التاجر بصفة دورية و منتظمة.

وجود نظام يمنع التلاعب في البيانات.[1]

و قبلت المحاكم الأمريكية المستندات الالكترونية في الإثبات فيما تعلق بالمسائل المدنية و التجارية – إذا توافر فيها شرط الانتظام و كانت صادرة في المجال التجاري – بوصفها أوراقا تجارية.[2]

الفرع الأول : شروط قوة الإثبات للمخرجات الالكترونية أمام القاضي الجنائي:

في إطار حماية القاضي لحقوق الأطراف فإن التشريعات وضعت ضوابط تحكم الأدلة المستخرجة آليا، هذه الضوابط مدارها أصل البراءة حيث لا مجال..... هذا الأصل و افتراض عكسها إلا بما يقتنع به القاضي اقتناء جازما و يقينا و على ذلك لا يقضي بالإدانة على المتهم المعلوماتي ما لم تصل قناعة القاضي إلى ذلك الحد و إلا فالبراءة محكمة[3].

لكن لنا أن نتساءل ما الذي يمكن للقاضي من أن يصل إلى حد الجزم و اليقين و هو يستند في إقرار حكمه و بناء قناعته على مستخرجات بنية الثقة فيها..... فهل وجدت هناط ضوابط ترفع نسبة قوة الاعتداد بهذه الأدلة ؟

حدد البعض[4] ضوابط لذلك تمثلت في ثلاث مبادئ:

مبدأ يقينية المخرجات الالكترونية

مبدأ وجوب مناقشة المخرجات الالكترونية

مبدأ مشروعية المخرجات الالكترونية

01- مبـــدأ يقينيـــة المخرجـــات الالكترونيـــة:

يقين القاضي هو مصدر ثقة الأفراد في العدالة، إذ لا يمكن التسليم بالحقيقة (القضائية) ما لم يتوفر اليقين فيها أصلا، و هذا اليقين هو ضمان سلامة إصابة القاضي في الحكم الذي يصدره[5]حيث لا يمكن إقامة الإدانة على مجرد الظنون و التخمين بل يجب أن تكون عقيدة القاضي على درجة عالية من الثقة فيما يؤسس عليه حكمه.[6]

---

[1] - من حق المتهم أن يثبت أن برنامج التشغيل لا يعمل بطريقة صحيحة و سليمة.

[2] - شيماء عبد الغني ، مرجع سابق ، ص، ص 408.

[3]

[4] - هلالي عبده ، مرجع سابق ، ص، الحجية، ص 71.

[5] - هلالي، الحجية، 70- 71.

[6] - هلالي، الحجية، 85.

و يصل القاضي إلى تحقيق..... المخرجات الالكترونية بطريقتين:

- **أولهما:** المعرفة الحقيقية من خلال معاينة المستخرج و تفحصه.
- **ثانيهما:** المعرفية العقلية عن طريق التحليل و الاستنتاج.

و تعني اليقينية في هذه المخرجات أن تكون دقيقة و ناتجة عن نظام يشتغل بصورة سليمة و صحيحة و لهيئة المحكمة أن تستعين بعامل الخبرة في ذلك لما لطبيعة هذه الإجراءات من عنصر التخصيص و الدقة و العلم.

02- مبـــدأ وجـــوب مناقشـــة المخرجـــات الالكترونيـــة:

هذا المبدأ يرتكز على مبدأ أصل في المحاكمة ألا و هو..... الجلسات فلضمان حقوق الأطراف و تحقيقا للعدالة ينبغي أن تعرض أمام الخصوم كما القاضي أدله التقاضي و من حق الأطراف ليس فقط الإطلاع على ما يستند عليه كل طرف في تقاضيه ضد خصمه بل و يحق له حتى مناقشة ما يطرح من أدلة و من حقه أيضا أن تتاح له الفرصة لإثبات أن الدليل المقدم مطعون فيه مثلا له الحق أن يثبت أن برنامج التشغيل لا يعمل بطريقة صحيحة أو منتظمة.[1]

و يترتب على هذا المبدأ أثران هما:

عدم جواز أن يقضي القاضي في الجرائم الالكترونية بناء على معلوماته الشخصية أي بناء على ما رآه بنفسه أو حققه في غير مجلس التقاضي بدون حضور الخصوم لما في ذلك مناقضة لقاعدتي الشفوية و المواجهة في مرحلة المحاكمة.

عدم جواز أن يقضي القاضي الجرائم المعلوماتية بناء على رأي الغير.

03- تسلـــح القاضـــي الجنائـــي بتقنيـــة و علـــوم الحاســـب:

أتاحت شبكة الإنترنيت سوقا واسعا أمام مئات الملايين من التجار و المستهلكين، و يسرت سبيل الحصول على السلع و الخدمات دون الحاجة للانتقال أو تطلب وسائل مادية، بل تمر أغلب عمليات و العقود عبر الشبكة ذات الطابع الدولي يتداخل في إطار هذه العلاقة التعاقدية أشخاص متواجدون و منتمون إلى دول مختلفة، فأطراف العقود التجارية المبرمة عبر الإنترنيت هم مستخدم مقيم في دولة، و مورد خدمات الاشتراك (تقدم الخدمات الوسيطة) في الشبكة من دولة ثانية، و شركة معالجة البيانات و إدخالها و تحميلها من دولة ثالثة فالبيانات و المعلومات التي إدخالها و تحميلها على الشبكة..... في ثوان في كل الدول المرتبطة بالشبكة حيث يمكن يتاح لكل مستخدم الدخول إلى هذه المعلومات و البيانات.[2]

---

[1] - شيماء عبد الغني ، مرجع سابق ، ص، ص 410.

[2] - حجازي، التجارة الالكترونية في القانون العربي النموذجي، مرجع سابق، ص 303.

و هذا الطابع الدولي غير مقتصر على العقود و بل منسحب حتى على سائر مراحل العملية التجارية كالدعاية و الترويج و السلع و الخدمات و غيرها.

و هذه العمليات لا يتوفر بشأنها معيار قانوني موحد هذا الطابع الدولي يخلف العديد من المشكلات بالنسبة للحماية الجنائية [1] للتجارة الالكترونية فيما يتعلق بتحديد المحكمة المختصة بالنظر بالمنازعات التي تنشأ عن المعاملة التجارية الالكترونية بالإضافة إلى مشكلة القانون الواجب التطبيق عليها.

مهم أن نقول أن نظرية الاختصاص أوسع نطاقا من أن تحضر في مجال المحاكمة ذلك أن قاعدة الاختصاص هي التي تحدد فن عمل القاضي من الأساس لأن الاختصاص هي التي تحدد فن عمل القاضي من الأساس لأن الاختصاص هو السلطة التي يقر بها القانون للقضاء في النظر في دعاوى معينة و الفصل فيها، و تحديد اختصاص سلطات الاتهام و التحقيق و سلطات جمع الاستدلالات [2] و على هذا الأساس قضت القاعدة التقليدية بوجوب القبول بدخول الدعوى في اختصاص محكمة معينة إذا كانت هذه الدعوى داخلة في اختصاص القضاء الإقليمي لدولة تلك المحكمة، و يعقد لها الاختصاص حتى ثبت الاختصاص الدولي للمحاكم الوطنية و إن كان المتهم شخصا أجنبيا.[3]

لكن هل يمكن انطباق هذه القاعدة على جرائم التجارة الالكترونية ؟

و الذي يدفع لطرح هذا الإشكال هو استحداث مراكز لم يكن للنصوص التقليدية إمكانية من توفير الحماية لها بفعل ورود المعطى الجديد على مستوى آلية التعامل التجاري التي حققت عنصر المفاجأة للمشرع.

ندرس هذا الإشكال من جانب تطرقنا لقواعد الاختصاص.

<u>قواعد الاختصاص المتعلقة بجرائم التجارة الالكترونية في بعض التشريعات:</u>

تكمن مشكلة اختصاص النظر في دعوى النظر في جرائم التجارة الالكترونية في كون أن شبكة الانترنيت التي تعتمدها التجارة الالكترونية توفر الحرية و قلصت الرقابة على التعاملات حيث ليست هي تحت سيطرة دولة معينة، ما يرتب عدم وجود قانون جنائي معين أو موحد يحكم هذه الشبكة بل إن القوانين السيادة الدولية [4] كما أن مفهوم النشاط الجرمي يقترن أو يرتبط في الجرائم الالكترونية بمفاهيم الإباحة و التجريم لكل دولة.[5]

---

[1] - أحمد عبد الكريم سلامة، الانترنيت و القانون الدولي الخاص،ص 29.

[2] - جميل عبد الباقي الصغير، الجوانب الإجرائية للجرائم المتعلقة بالانترنيت، دون طبعة، دار النهضة العربية، 2002، ص 42.

[3] - عمر محمد أبوبكر بن يونس ، مرجع سابق ، صعبد الأحد، ص 898.

[4] - جميل ، الإجراءات، ص 43

[5] - عمر محمد أبوبكر بن يونس ، مرجع سابق ، ص ص 905.

فالمشكلة التي تشترك فيها جرائم التجارة الالكترونية مع غيرها هي جرائم الانترنيت هو "تدويل لجرائم المرتكبة" لكون السلوك المجرم يمر عبر عدة دول مع غياب رقابة على الشبكة، و انتفاء وجود قانون محكمة و محدد يحكمها فإلى أي مدى يمكن تطبيق القوانين الوطنية على مثل هذه الجرائم ؟.[1]

بالنسبـــة للقضـــاء الأمريكـــي:

يعتمد القضاء الأمريكي منهجا يحدد بمقتضاه مدى إمكانية اختصاص بالنظر إلى قضايا وقعت خارج الولايات المتحدة الأمريكية و هذا المنهج يرتكز على:[2]

إلزام القضاء البحث عن نسبة الكونجرس فيما يتعلق بامتداد تطبيق التشريع الأمريكي المجرم للواقعة إلى وقائع ارتكبت خارج الإقليم.

يلزم بتقرير ما إذا كانت نتائج النشاط المحدد في التشريع تبرر القول بالاختصاص و لم يكن هذا التطور التشريعي كامنا ليطال جرائم التجارة الالكترونية بما دعى إلى وجود منهج آخر في هذا الشأن، و في سنة 1986 صدر قانون مكافحة الإرهاب تضمنت نصوصه ابتداء الاختصاص القضائي الأمريكي بالنظر في الجرائم الواقعة في الخارج.[3]

و في عام 1999 قرر القضاء الأمريكي تأسيس قاعدة الاختصاص على قاعدة اعتماد مكان مرتكب الجريمة و ليس المكان الذي يتواجد فيه مزود خدمات الانترنيت،

كما اعتمد مبدأ آخر أبرز مدى توسع المشرع في الولايات المتحدة الأمريكية في امتداد اختصاص محاكمها الجنائية بمبدأ النتيجة الإجرامية فأعطى الاختصاص للمحاكم الجنائية (إذا حدثت آثار الجريمة على إقليمها). [4] و يعرف بمبدأ الاختصاص بالنتيجة The effécts principal حيث يتضمن المبدأ الأثر الامتدادي للنتيجة الإجرامية.[5]

---

[1] - جميل عبد الباقي الصغير ، مرجع سابق ، ص، الجوانب الإجرائية، ص 44.

[2] - جميل عبد الباقي الصغير ، مرجع سابق ، ص، الجوانب الإجرائية، ص 905، مرجع سابق.

[3] - إبان نشر فكرة امتداد الاختصاص القضاء الأمريكي إلى الجرائم الواقعة خارج الإقليم الأمريكي بدافع حماية الأمن القومي و لو كان السلوك الضار بالمصالح الأمريكية واقعا خارج الإقليم الأمريكي، عمر محمد أبوبكر بن يونس ، مرجع سابق ، ص ص 906.

[4] - غير أنه هناك اختلاف بين المحاكم الأمريكية فيما يتعلق بتحديد معيار الاختصاص بالجرائم المعلوماتية من ولاية إلى أخرى فبتعدد هذه الولايات تتعدد هذه المعايير (معيار وجود الجهاز المستخدم في ارتكاب الجريمة معيار مكان وقوع الضرر مكان وجود المتحصلات الناتجة عن الجريمة و الوسائل المستخدمة في ارتكابها معيار مكان حدوث الدخول على الجهاز بدون وجه حق أو على الشبكة إذا وقع على إقليم الدولة أو من خلالها، مكان الدخول إلى جهاز الكمبيوتر و كذلك محكمة مكان وجود الكمبيوتر الذي يتم الدخول إليه بدون وجه حق مادة 21/1957 ولاية أو كلاهما) معيار مكان البث، يرجع إلى الكتاب لتحديد الولايات، شيماء عبد الغني ، مرجع سابق ، ص، ص 373.

[5] - عمر محمد أبوبكر بن يونس ، مرجع سابق ، ص ص 907-908.

أما المشرع الفرنسي فقد توسع منفرد عن غيره حيث ميز بين في إطار سعيه إلى تطبيق قواعد الاختصاص القضائي في تشريعاته – تلك الجرائم التي وقعت داخل فرنسا و بين الجرائم التي وقعت في فرنسا –

فقد عقب الاختصاص للقضاء الفرنسي بشكل طبيعي بالنسبة لتلك الجرائم التي وقعت داخل الإقليم الفرنسي فيما قضت به المواد 1/113 إلى 5/113 من قانون العقوبات الجديد.[1]

و يترتب على أحكام هذه المواد القول بأن القانون الفرنسي تسحب فيه قواعد الاختصاص على جرائم التجارة الالكترونية طالما أنه الاختصاص ينعقد لمجرد وقوع أحد العناصر المكونة للجريمة. أو وقوع النتيجة على هذا الإقليم فمتى كانت الجرائم الواقعة خارج الإقليم مرتبطة ارتباطا وثيقا لا يقبل التجزئة مع جرائم وقعت على الإقليم الفرنسي.[2]

كما قد نصت عليه المادة 2/113 تدع هذه يطبق القانون الفرنسي على الجرائم المرتكبة على إقليم الجمهورية، و تعتبر الجريمة قد ارتكبت على إقليم الجمهورية إذ كان أحد عناصر الجريمة قد وقع على هذا الإقليم.[3]

هذا ما يجعل القانون الموضوعي الفرنسي ينطبق بشكل تلقائي مما يستدعي ضرورة تطبيق القانون الإجرائي[4] بالرغم من المادة 5/113 ربما كانت الأكثر توسعا في مد الاختصاص لهذه الجرائم بنصها على أنه القانون الفرنسي يطبق على كل من ارتكب فعل إقليمها يجعله شريكا في جناية أو جنحة وقعت في الخارج إذ كانت الجناية أو الجنحة معاقبا عليها في القانون الفرنسي و القانون الأجنبي، و كانت ثابتة بمقتضى حكم نهائي من القضاء الأجنبي و هذا ما يمكن من تطبيقه على أغلب جرائم التجارة الالكترونية.[5]

– كما أنه قد عقد الاختصاص القضائي في حالة إذا كانت الجريمة واقعة خارج فرنسا وفق ما قررته المادتان 06/113 و 07/113 من قانون العقوبات الفرنسي الجديد إذ كانت ظروف الواقعة أو عينة الواقعة تجعل من تطبيق القانون الفرنسي مصلحة لفرنسا و بذلك تكون فرنسا هي صاحبة الاختصاص، القضائي في المحاكمة.[6]

و قد أخذ المشرع الفرنسي بمبدأ الشخصية النص الجنائي بوجهيه السلبي و الإيجابي و نستعرضها كالآتي[7] حيث بالنسبة للوجه الإيجابي نصت المادة 06/113 من قانون العقوبات

---

[1] - عمر محمد أبوبكر بن يونس ، مرجع سابق ، ص ص 912.
[2] - شيماء عبد الغني ، مرجع سابق ، ص عبد الغني، ص 369.
[3] جميل عبد الباقي الصغير ، مرجع سابق ، ص، الجوانب الإجرائية، ص 47، النص بالفرنسية.
[4] - عمر محمد أبوبكر بن يونس ، مرجع سابق ، ص ص 912.
[5] - جميل، الجوانب الإجرائية، 50-51.
[6] - عمر محمد أبوبكر بن يونس ، مرجع سابق ، ص ص 913.
[7] - جميل عبد الباقي الصغير ، مرجع سابق ، ص، الجوانب، ص 56، النص الفرنسي.

الفرنسي الحديث عل أن القانون الفرنسي يطبق على جناية يرتكبها فرنسي خارج إقليم الجمهورية، و يطبق هذا القانون أيضا على الجنح التي ترتكبها فرنسي خارج فرنسا إذا كانت الوقائع المكونة لها معاقب عليها في قانون الدولة التي ارتكبت فيها و أحكام هذه المادة تطبق حتى و لو كان المتهم قد اكتسب الجنسية الفرنسية بعد ارتكاب الواقعة المنسوبة إليه.[1]

و بالنسبة للجانب السلبي فقد سمح بحماية الفرنسي سواء كان شخصا طبيعيا أو كان شخصا اعتباريا إذا وقع عليه ضرر و لو كان الجاني أجنبيا أو فرنسيا أو ارتكبت هذه الجناية في الخارج.

و يترتب على إعمال توجيه المشرع الفرنسي في قانون العقوبات الجديد أن تطال النصوص العقابية باختصاصها تلك الجرائم التي تصنف ضمن الجرائم الواقعة على التجارة الالكترونية و لو ارتكبت في الخارج على إقليم دولة أجنبية إذا ارتكبت ضد مواطن فرنسي بالاختصاص هنا منعقد للمحاكم الفرنسية بنص المادة 07/113 التي نصت على أن القانون الفرنسي يطبق على أية جناية أو جنحة يعاقب عليها بالحبس ارتكبها فرنسي أو أجنبي في الخارج إذا كان المجني عليه فرنسيا لحظة ارتكاب الجريمة.

أمـــا القضـــاء الانجليـــزي:

فإن قانون إساءة استخدام الحاسوب فقد قرر في مادتين [2] إلا أنه توجد هناك قيود تمنع تحريك الدعوى الجنائية عن هذه الجرائم التي تقع في الخارج، حيث لا ينعقد الاختصاص للمحاكم الفرنسية بشكل تلقائي بالنسبة للجرائم التي تقع في الخارج، فلا يجوز تحريكها دون معرفة النيابة العامة و هذا حسب منطوق المادة 8/113 من قانون العقوبات الفرنسي الجديد التي أكدت على أنه في الجرائم المنصوص عليها في المادتين 113-6/113-7 لا ترفع الدعوى الجنائية إلا بناءا على طلب من النيابة العامة، مع وجوب أن يكون هذا الطلب مسبوقا بشكوى من المجني عليه أو من خلفه أو بناءا على بلاغ رسمي من سلطات الدولة التي وقع الفعل على إقليمها.[3]

كما وضعت المادة 9/113 قيدا آخر و هو عدم جواز محاكمة الشخص عن الفعل الواحد مرتين حيث أكدت على أنه في الحالات المنصوص عليها في المادتين 6/113 و 7/113 لا تقام الدعوى الجنائية ضد شخص ثبت أنه حوكم نهائيا في الخارج عن نفس الوقائع و ثبت في حالة

---

[1] - 56، نص الفرنسية.

[2] - The Computer Misuse Act Of 1990:Sobsection 4/1,4/3

[3] - النص الفرنسي عند جميل 58، الجوانب.

الإدانة أنه نفذ من العقوبة أو أنها سقطت بالتقادم. [1]أن معيار اختصاص القضاء الانجليزي هو ارتباط الواقعة الإجرامية و بريطانيا سواء أكان مرتكب الجناية قد ارتكبها في بريطانيا دون أن يكون هو مقيما في بريطانيا المهم أن يكون ناتج عمله حصيلة تعديل غير مصرح به في بريطانيا، هذا هو معيار الاختصاص للمحاكم البريطانية للنظر في الدعاوى المنبثقة عن القانون السابق.[2]

كما حددت المادة الخامسة من ذات القانون اختصاص القضاء الانجليزي بالنظر في الجرائم المعلوماتية و فيها جرائم التجارة الالكترونية حتى و لو لم يحدث الفعل المؤثم على الإقليم البريطاني أو تواجد المتهم على هذا الإقليم.

و يقصد بالعلاقة القوية وفقا لهذه المواد المذكورة في قانون 1990 أن يتواجد المتهم الذي نفذ الجريمة في بريطانيا مادام أنه استخدم جهاز الكمبيوتر في بريطانيا.

و ينعقد الاختصاص للقضاء البريطاني إذا كان الجهاز الذي دخل عليه المتهم بدون وجه حق أو كان يقصد الدخول إليه متواجدا على إقليم بريطانيا.[3]

و بالنسبـــة لتشريعـــات أخـــرى:

أخذت بعض التشريعات بمبدأ العالمية في تحديد اختصاص قضائها الجنائي الوطني و فيها دولة الإمارات العربية المتحدة حيث قضت بأن الاختصاص ينعقد لمحاكمها تبعا لمبدأ العالمية في جرائم معينة [4]، و المقصود بهذا المبدأ هو أن المحاكم الوطنية تختص بمحاكمة مرتكبي بعض الجرائم بالرغم من وقوع هذه الجرائم في خارج إقليم الدولة و أن المتهمين أو الجناة ليسوا من مواطني هذه الدولة و العبرة في توسيع و حد هذا الاختصاص هو أن الجريمة ذات طبيعة دولية تخل بقيم المجتمع الدولي.

و من هذه الجرائم ما تعلق بجرائم الاتجار الالكتروني غير المشروع أو جرائم تعطيل أو تخريب وسائل الاتصال، و نهج المشرع البلجيكي مثل هذا الاتجاه.[5]

---

[1] - جميل عبد الباقي الصغير ، مرجع سابق ، ص، الجوانب، النص بالفرنسية، ص 59.

[2] - عمر محمد أبوبكر بن يونس ، مرجع سابق ، ص ص 911.

[3] شيماء عبد الغني ، مرجع سابق ، ص عبد الغني، ص 379.

[4] - نصت المادة 21 من قانون العقوبات الإماراتي على أنه " تطبق مبدأ العالمية في الجرائم التالية:
- جريمة تخريب أو تعطيل وسائل الاتصال الدولية
- جريمة الاتجار بالمخدرات
- جريمة الاتجار بالرقيق الأبيض (البغاء)
- جريمة الاتجار بالصغار و الرقيق
- جريمة القرصنة
- جريمة الإرهاب الدولي"

[5] - أنظر شيماء عبد الغني ، مرجع سابق ، ص عبد الغني، ص 368.

نشير إلى أن مكان البث يولي له القضاء أهمية بالغة من ذلك، إن محكمة ولاية Missouri قضت باختصاصها بنظر قضية تقليد علامة تجارية مع أن المتهم يقيم بولاية كاليفورنيا استنادا إلى مكان موقع البث و أنه يكفي أن يستطيل البث إلى ولاية Missouri لكي ينعقد الاختصاص لمحاكمها.[1]

.....

المطلب الثالث : خصائـــص الدليـــل الالكترونـــي

تفيد دراسة خصائص الدليل الرقمي في استجلاء حقيقته على النحو الذي يحثث إمكانية التعامل القانوني معه[2] هذا التعامل هو مفروض بحتمية الانخراط في العالم الافتراضي بكل منظوماته و التجارة الالكترونية أقوى هذه المنظومات و أهم خصائصه هي:[3]

الفرع الأول : كـــون الدليـــل الالكترونـــي علمـــي:

هو دليل يحتاج إلى قدر من التمكن من آليات بيئته التقنية التكنولوجية فهو يصنف ضمن دائرة الأدلة العلمية و هذه الخاصية و إن تبدى للوهلة الأولى عظم إيجابياتها حيث انضباط التعامل مع هذا النوع من الأدلة لمعايير علمية مضبوطة إلا أن ذات الإيجابية هي إشكالية بحد ذاتها لكون الدليل الرقمي حين ارتفعت فيه درجة الضبط أصبح متسارع التغير، حيث التحديث في عالم الرقمية تحديث لحظي أي لا يكاد يستقر من حيث الزمن ما يعني عدم وجود قواعد جامدة يرتبط بها الدليل الرقمي من حيث طبيعته العلمية.

و مشكلة أخرى تطرحها هذه الخاصية هي تقلص دور القاضي في التعامل مع هذا الدليل حيث عادة ما يلجأ القاضي الجنائي إلى الاستعانة بالخبرة أمام قضايا تتعلق فيها الأدلة بالبيئة الرقمية و ينعكس هذا الأمر على أحكام القضاء في تراجع دور القاضي إلى مجرد ناقل لرأي الخبير دون معرفة محتوى الخبرة أو موضوعها و تقدير الحكم حولها.[4]

الفرع الثاني : الدليـــل الالكترونـــي مـــن طبيعـــة تقنيـــة:

---

[1] - شيماء عبد الغني ، مرجع سابق ، ص عبد الغني، ص 376.
[2] - عمر بن يونس، مرجع سابق، ص 977.
[3] - عمر بن يونس، مرجع سابق 977- 983.
[4] - نسرين يونس، ص 977.

لم تتكيف التشريعات بعد للتعامل مع مستخرجات التقنية مثلما أنها لم تحز ثقتها بعد و لحد تألف التعامل معها حتى فلا تزال التشريعات أو بعضها لا تنزع للاعتداد بهذا النمط من الأدلة لكونه ذو طبيعة تقنية معنوي افتراضية محصلة في الأخير نبضات كهربائية أو عبارة عن أرقام تستعص على كثيرين قواعد الإجراءات الجنائية مثل التفتيش و الضبط و غيرها فضلا عن عدم أهلية الأجهزة القضائية للتعامل مع هذه الأدلة [1] ما..... المشرع البلجيكي إلى ان يعدل قانون التحقيق الجنائي لديه بإضافة المادة (bic 39) التي سمحت بضبط الأدلة الرقمية كنسخ المواد المخزنة في نظام المعالجة الآلية للبيانات قصد عرضها على الجهات القضائية و كان ذلك بمقتضى قانون 28 نوفمبر 2000.[2]

الفرع الثالث : تنـــوع الدليـــل (الرقمـــي) الالكترونـــي وتطوره :

بالنسبة للتنوع فإن مصطلح الدليل الرقمي مصطلح تتسع حدوده و لا تضيق فهو يشمل كافة أنواع البيانات الالكترونية الممكن تداولها و اعتمادها في المعاملة التجارية من جهة و إمكانية قيام رابطة ما بينها و بين الجريمة من جهة ثانية و أخيرا إمكانية اتصالها بالجاني من جهة ثالثة، هذه البيانات يمكن أن تأخذ محتواها شاكلة النصوص، الصور، سمعيات، مرئيات، مخططات و غيرها من البيانات التي تصلح أن تكون محلا لسلعة أو خدمة تجارية هذا من ناحية التنوع ، أما بالنسبة للتطور فلقد فقد منتجو الثورة التكنولوجية السيطرة عليها فالتكنولوجيا لا تنتظر أصحابها و منشأها فضلا عن مستهلكيها حيث هذا التطور تلقائي آلي و ما يستحدث اليوم هو بال في مساء يومه فالعالم الرقمي لا تبدو له حدود نهاية و لا تتضح له ملامح تحدد أطره و ليس من السهولة احتواءه.[3]

الفرع الرابع :استرجـــاع الدليـــل (الرقمـــي) الالكترونـــي:

توجد هناك مجموعة

---

[1] - قد يحدث و أن يتلف الدليل فإساءة البحث عنه و جهل كيفية التعامل معه.

Éric A. CAPRIOLI, Mesures techniques de protection et d'information des droits d'auteur, Revue Revue **Communication Commerce électronique n° 11, Novembre 2006, Etude 30**

[2] - عمر بن يونس، ص 978.

[3] - عمر بن يونس، ص 980.

تختلف التشريعات حول مسألة قبول الدليل الالكتروني تبعا لخصوصية أولا و بحسب النظام الإجرائي الذي تعتمده كل تشريع و نظام الإثبات المقر حسب ما سنرى، لكن نستطيع أن نخص بعض الشروط العامة الواجب توفرها في الدليل الالكتروني المقدم:[1]

أن يكـــون الدليـــل الالكترونـــي لـــه علاقـــة بموضـــوع الدعـــوى:

طالما أن للدليل الالكتروني المقدم علاقة بموضوع الدعوى يتحقق أول شرط بقبوله حيث يقضي باستبعاد كل دليل لا يتعلق بموضوع الدعوى أو ليس من شأنه الكشف عن الحقيقة أو الإسهام في الوصول بواسطته إلى الجاني.

الصحـــة و المطابقـــة:

نصت المادة 69 من قانون الشرطة و الأدلة الجنائية 1986 على أنه في أي مرحلة من مراحل الإجراءات الجنائية لا يقبل البيان المتضمن في مستند الكتروني أو مستخرج من حاسب آلي كدليل عن أي واقعة ما لم يتبين أنه ليس هناك إدعاء يصلح كأساس للاعتقاد بأن البيانات غير دقيقة بسبب عدم دقة الحاسوب.[2]

التوافـــق مع الأدلـــة التقليديـــة:

تستند الأدلة الالكترونية بدعمها بأدلة تقليدية في ذات الوقت و يكون لكل فيها..... بوجود الآخر.

المبحث الرابع : دور القاضـــي فـــي تقييـــم أدلـــة الجرائـــم المعلوماتيـــة:[3]

المطلب الأول : مـــدى صلاحيـــة جرائـــم الحاســـب الآلـــي لضبـــط أدلتـــها:

قد يكون الأمر مفصولا فيه إذا ما روعي أو نظر لإجراء الضبط في بيءة المعلوماتية إذا ما تعلق الأمر بالجرائم الواقعة على المكونات المادية للحاسب، فهذه الحالة لا تثير أية صعوبة للتقرير بصلاحية هذه الجرائم لضبط أدلتها بموجب قواعد التفتيش التقليدية التي لا يرد فيها هذا الإجراء إلا على أشياء مادية و معدات الحاسب الآلي و مفاتيح التشغيل و الدعامات المادية و

[1] - عمر بن يونس، ص 992- 994.
[2] - شيماء 391، عمر بن يونس 993.
[3] - يرجع إلى عفيفي كامل، ص 364.

الأشرطة و الأقراص و الاسطوانات و غيرها هي مكونات مادية لكن الإشكال يطرح حول مدى صلاحية إجراء الضبط إذا ما تعلق بالمكونات غير المادية للحاسب الآلي ؟

و لعل البرامج و البيانات هي موضوع الإشكال.[1]

الملاحظ أن قوانين الإجراءات الجنائية في التشريعات المقارنة لم تورد نصا خاصا بقواعد إجراءات الضبط في بيئة التجارة الالكترونية دون أن يكون هناك ما يمنع أو يحول دون تطبيق النصوص التقليدية لقواعد الضبط على جرائم التجارة الالكترونية أي أنه في غياب نصوص خاصة متعلقة بالنواحي الإجرائية الخاصة بالبيئة الالكترونية فإنه ليس أمام الجهات المختصة بالتحقيق إلا إعمال القواعد العامة التقليدية في الضبط على المعلومات[2]

مادام أنها تشكل موضوع جريمة أو أنها من متحصلات الجريمة أو أنها تفيد في إثبات دليل أو كشف حقيقة.[3]

الفرع الأول :بالنسبـــة لبرنامـــج الحاســـب:

تبرز إشكالية البرامج هنا إذا ما استخدمت وسائل تقنية في إتلافه و يكون ذلك بواسطة زرع فيروس لتدمير ذلك البرنامج و هذه الصعوبة ترجع إلى قلة خبرة جهات الضبط بتقنية المعلوماتية لقلة التدريب أو ضعف الخبرة [4]و بسبب ثاني متمثل في أنه إذا تمت عملية الضبط لهذه الوسائل التقنية في الأنظمة المعلوماتية الكبيرة أو الشبكات الكبيرة و عادة ما تكون كذلك في مجال معاملات التجارة الالكترونية[5] فإن صعوبتين تعترضان هذا الإجراء هما:[6]

1 – إجراء الضبط قد يؤدي إلى عزل النظام المعلوماتي بالكامل عن دائرته لمدة زمنية و هو ما يعني إلحاق ضرر بالجهة مستخدمة النظام، يتعين في هذه الحالة إعمال مبدأ التناسب أي اقتصار الضبط على الأدلة التي تفيد في كشف الحقيقة حتى لا يترتب على إجراء الضبط تعطيل عمل النظام[7] و الشبكات المتصل بها مما يعني توقف عمل المشروعات

---

[1] - عفيفي كامل، جرائم الكمبيوتر، ص 253 / حجازي، الإجراءات، ص 211- 218.

[2] - تسمح المحاكم الأمريكية بضبط المعلومات بالرغم من كون المادة 41 من قانون الإجراءات الجنائية الفدرالي متعلقة بتفتيش و ضبط الأشياء المادية، كما أن قانون الإثبات في بريطانيا يتضمن نصوص تسمح بضبط المعلومات الموجودة في الحاسب الآلي، شيماء 357.

[3] - شيماء، ص 357.

[4] **Éric A. CAPRIOLI, Transparence et sécurité des informations financières par voie électronique dans le règlement AMF après l'arrêté du 4 janvier 2007,** Revue **Communication Commerce électronique n° 6, Juin 2007, comm. 87**

[5] - حجازي، مبادئ الإجراءات، ص 211- 213.

[6] - عفيفي كامل، ص 354.

[7] - شيماء، ص 358.

صاحبة النظام حيث الأعطال تقاس بالثواني و الأعشار لما يمكن أن يترتب عليها في الأخير مبالغ مالية معتبرة.

2 - ..... مستخدمي الأنظمة المعلوماتية عن التعاون مع الجهات القضائية في هذه المرحلة بما له في نظرهم من مساس بمراكز قانونية (أسرار جهته، بيانات متعاملين، سر تجاري أو مهني، خصوصية، سر مهني متعلق بميزات تنافسية تجارية...).

الفرع الثاني : بالنسبـــة لبيانـــات الحاســـب الآلـــي

يمكن أن نحصر صعوبات أو إشكاليات الضبط في هذا المجال أي التي تعترض سبيل المحقق أثناء ضبطه للبيانات التي تعد دليلا على ارتكاب الجريمة في بيئة المعاملات التجارية الالكترونية و هي:[1]

- عدم وجود دليل مرئي يمكن فهمه و هذا معوق لعمل المحقق.
- عدم ترك أي آثار يمكن الاستدلال بها حال ارتكاب جرائم من هذا الصنف (اختلاس، تزوير).
- إمكانية فقد الدليل بعد ضبطه بواسطة برنامج يعده الجاني سلفا و قد يكون ذلك بثوان بعد عملية الضبط.[2]
- ضخامة كم البيانات المضبوطة من أجل الفحص من قبل المحقق الجنائي، و وجود بيانات محمية فنيا تنظم حماية و أمن أو تطبق للوصول إلى بعض البيانات إلى كلمات سر أو شفرات ترميز.
- عدم تناسب قواعد الضبط و التحرير التقليدية مع نوع الأدلة في هذه الجرائم و التي ينتفي عنها الطابع المادي و مع ضعف تدريب المحققين على الإجراءات الفنية يكون سلامة و الحفاظ على الأدلة معرضة للفقد.

و مع عدم وجود مدرسين مؤهلين للتعامل مع البيانات التي هي دليل لجريمة الكترونية بأن مع ضعف تدريب المحققين على الإجراءات الفنية، فإن الدليل الرقمي الالكتروني يكون مهد في سلامته و مدى الحفاظ عليه مما يجعله عرضة للإغفال أو الإهمال أو الإتلاف أو إفساده.

المطلب الثاني : موقـــف الفقـــه المقـــارن مـــن ضبـــط الأدلـــة فـــي مجـــال المعالجـــة الآليـــة:

---

[1] - عفيفي كامل، ص 355 / حجازي، الإجراءات، ص 213-218.

[2] - لذلك ينصح بعدم البدأ بتشغيل البرامج المضبوطة إلا بعد أن يتم تأمينها فنيا لضمان سلامتها و أخذ نسخة منها، عفيفي، ص 361 / حجازي، الإجراءات، ص 225.

الفقـــه المقارن و ضبـــط الأدلـــة المعلوماتيـــة:[1]

حول مدى صلاحية إجراء الضبط و في الجرائم الالكترونية و إعمال هذا الإجراء على البيانات و البرامج حال كونها مجردة من دعامتها المادية اختلف الفقه المقارن إلى ثلاث اتجاهات:[2]

الفرع الأول : الاتجـــاه الأول:

تبعا لانتفاء الطابع المادي عن البيانات و البرامج حال تجردها عن الدعامة المادية فإن أصحاب هذا الاتجاه يرون عدم صلاحية هذه البيانات و البرامج لأن تكون محلا للضبط بأحكام النصوص التقليدية و يحبذ هذا الاتجاه الفقه الألماني و لوكسمبورج.[3]

الفرع الثاني : الاتجـــاه الثـــاني:

يرى هذا الاتجاه صلاحية البيانات و لا يوجد من يمنع من ذلك و أصحاب هذا الاتجاه هم الفقه الكندي و الأمريكي مستندين في ذلك على نصوص تشريعاتهم بالفقرة السابعة من المادة 29 من قانون الإثبات الكندي تنص على أن "ما لم يرد ما يخالف ذلك في أمر التفتيش و ضبط الدفاتر و السجلات الخاصة بمؤسسة مالية... يقتصر التفتيش على المكان بغرض تفقده و أخذ نسخ من المواد المكتوبة و ينطبق هذا النص سواء كانت السجلات مكتوبة في شكل الكتروني...".[4]

الفرع الثالث : الاتجـــاه الثـــالث:

يدعو لتدخل المشرع لأجل أن يوسع من نطاق الأشياء الممكن ضبطها للأشياء ذات الطابع المعنوي المفتقدة للطابع المادي، حيث يحكم أصحاب هذا الاتجاه أنه لا فائدة من محاولة تطويع النصوص التقليدية للضبط و تطبيقها على بيانات مجردة عن دعامتها المادية[5].

---

[1] - حجازي، الإجراءات، ص 218.
[2] - عفيفي كامل، ص 358- 359. / حجازي، الإجراءات، 218- 221.
[3] - قضت المحاكم الفدرالية قبلا بإلغاء إجراءات الضبط الواقعة على مثل هذه الأدلة، أنظر شيماء، ص 358.
[4] - أما سند الفقه الأمريكي فهو التشريع الخاص بما قبل المحاكمة الصادر عام 1975 للإصلاح على نص المادة، طالع عفيفي، ص 359 / حجازي، الإجراءات، ص 220.
[5] **Agathe LEPAGE, Libertés sur l'Internet et cybercriminalité : les apports au droit pénal de la loi pour la confiance dans l'économie numérique du 21 juin 2004, Revue Droit pénal n° 12, Décembre 2004, Etude 18**

الفصل الثالث

-الحماية الإجرائية في ضوء الاتفاقيات الدولية

-التعاون الدولي

ظهر الاهتمام الدولي بالحماية الجنائية في إطارها الإجرائي في ما تعلق بالجرائم الماسة بالتجارة الالكترونية في عدة اتفاقيات دولية لأجل التصدي للاستخدامات غير المشروعة لشبكة الانترنيت و الحاسبات الآلية و كان من أهم هذه الاتفاقيات:

مؤتمـــر ريوديجانيـــرو 1994:

انعقد هذا المؤتمر بمدينة ريوديجانيرو و هو المؤتمر الخامس عشر للجمعية الدولية لقانون العقوبات[1] و ذلك بتاريخ.... سبتمبر 1994 بالبرازيل لمناقشة أهم الموضوعات المستحدثة و التي يمكن أن تستحدث في إطار استغلال تقنية الرقمية في مجالات شتى و فيها معاملات التجارة الالكترونية، و لعل أهم المبادئ التي تعلقت بموضوع أهم المبادئ التي تعلقت بموضوع هذه الجرائم:[2]

[1] - سبق المؤتمر حلقة تمهيدية له عقدت على مستوى دولي في Wurz Bourg بألمانيا لبحث جرائم الحاسب الآلي و الجرائم الأخرى المتصلة بتكنولوجيا المعلومات في الفترة من 5- 8 أكتوبر 1992.

[2] - ابراهيم الدسوقي، ص485.

- وجوب وضع..... كافية (على أن تتعادل مع الحماية الكافية لحقوق الإنسان و حرمة الحياة الخاصة) تحت تصرف سلطات التحقيق و التحري في إطار ما يتطلبه التنقيب بالنسبة للجرائم من هذا النوع في بيئة تكنولوجيا المعلومات.
- يجب أن ترتكز تلك القيود التي ترد على حقوق الإنسان عن طريق رجال، السلطة على قانونية واضحة و دقيقة و تتوافق مع المعايير الدولية لحقوق الإنسان لتجنب تعسف السلطة الرسمية.
- يقع تحت طائلة البطلان كل دليل يتحصل عليه رجال و السلطة العامة بطريق تنتهك فيها حقوق الإنسان بالإضافة إلى تقرير المسؤولية الدولية الجنائية لرجل السلطة العامة التي انتهك القانون.

يتضح من خلال هذه المبادئ مدى الأهمية التي أولها المؤتمر لنطاق حماية حقوق الإنسان و الحياة الخاصة أنه هذه الحقوق محمية من طريقين.

1 – تدويل حماية حقوق الإنسان في الاتفاقيات الدولية
2 – حرمة الحياة الحاضر حق دستوري فأكد عليه في كل التشريعات
3 – تحديد سلطات جهات التفتيش و الضبط في إطار تحريها عن جرائم المعاملات التجارية الالكترونية لأنها تتعامل مع كيانات غير مادية.
4 – بيان حدود واجبات مزودي الخدمات الوسيطية و الشهود و المجني عليهم في إطار التعاون مع رجال الضبطية القضائية و الجهات القضائية لأجل التحري عن هذه الجرائم و كشف الحقيقة.
5 – وجوب بيان الحد الذي يسمح من خلاله لسلطات و الجهات القضائية اعتراض الاتصالات أو الاطلاع على تسجيلات و بيانات نظم المعالجة الآلية و استخدام الأدلة التي يتم الحصول عليها في الإجراءات أمام المحاكم.

من المبادئ التي أقرها المؤتمر أيضا ضرورة إدخال تعديلات و بعض التغيرات التشريعية فيما يتعلق بموضوع الأدلة و في بيئة التحقيق في المعاملات الالكترونية و قبول مصداقيتها و إعطائها الحجية بما يمكن أن تثيره من مشاكل عند إسقاط الإجراءات الجنائية القضائية التقليدية و هذا العنصر هو أقرب إلى الدعوة إلى تحديث النظم الإجرائية الحالية بما يتوافق و خصوصية الإجراءات الموجهة للحماية أو التصدي بمثل هذه الجرائم بالأخص فيما يتعلق بنصوص التفتيش و ضبط نظم المعالجة الآلية و نظم الحاسب الآلي.

بالإضافة إلى أن هذا المؤتمر قد أوصى بحملة توصيات بلغ عددها 30 توصية كان أهمها:

- وجوب كفالة حقوق الإنسان في كل مراحل الدعوة الجنائية.[1]
- المتهم المعلوماتي تستفيد من قرينة البراءة في كل مراحل الإجراءات المتابعة و المحاكمة.[2]
- تطبيق مبدأ التناسب عند اتخاذ أي وسائل سرية في مرحلة التحقيق الابتدائي.[3]
- أي إجراء يتخذ من جانب الأجهزة القضائية يجب أن يكون..... من قبل القاضي أو خاضعا لرقابته إذا كان يمس بالحقوق الأساسية للمتهم (و فيها الإجراءات التي تتخذها الضبطية القضائية).[4]
- كل إجراء..... يتخذ من جانب سلطة التحري أو الشرطة يجب أن يصادق عليه القاضي في 24 ساعة.[5]
- لا تقبل وسائل و أدلة الإثبات التي تمس بدرجة خطرة بالحق في الخصوصية يسبقها إذن من القاضي و في الحالات التي قررها المشرع بطريقة واضحة.[6]

- اعتراف المتهم لا يقوده إلى الإدانة الجنائية بالضرورة دون فحص صدقه.[7]
- البحث عن الأدلة في المرحلة الابتدائية لا يصلح أن يستخدم كأداة للإدانة.[8]
- ضرورة احترام السر المهني أثناء البحث عن الأدلة.[9]
- تقع تحت طائلة البطلان و لا يمكن مراعاته في أي لحظة خلال الإجراءات كل دليل يتم الحصول عليه عن طريق انتهاك أو تعد على حق أساسي للمتهم.[10]
- قبول نتائج المراقبة الالكترونية عن بعد يجب أن تكون منظمة بواسطة القانون.[11]
- لا يقبل منح الإعفاء من العقاب أو تخفيف العقوبة لبعض الشهود أو بعض المرشدين الرسمين إلى بصفة استثنائية في القضايا الخطيرة أو الجريمة المنظمة، و لا يكون لإقراراتهم أي قوة في الإثبات إذا لم يعلن عن هوية هؤلاء الأشخاص.[12]

---

[1] - توصية رقم 1.
[2] - توصية رقم 2.
[3] - توصية رقم 02.
[4] - توصية رقم 10.
[5] - توصية 11.
[6] - توصية 12.
[7] - توصية 14.
[8] - توصية 13.
[9] - توصية 17.
[10] - توصية رقم 18.
[11] - توصية 15.
[12] - توصية 16.

- لا يعبر أحد على أن يساعد في اتهام نفسه جنائيا بأسلوب إيجابي مباشرة أو بطريقة غير مباشرة.[1]

اتفاقيـــة بوداســـت 2001:

تعتبر هذه الاتفاقية جد هامة لما حوته من مجموعة مواد و توصيات و قد وقعت عليها ثلاثون دولة أوربية بما فيها دول غير أوربية مشاركة في الاتفاقية طبقا لنص المادة 36 منها و هي كندا، اليابان، جنوب إفريقيا، الولايات المتحدة الأمريكية.

و قد صدرت هذه الاتفاقية كون أن الدول الأوربية و الموقعة على هذه الاتفاقية تؤمن بأنه يجب على القانون أن يحافظ على مسايرته للتطورات التكنولوجية التي يمكن من إساءة استخدام آليات و إمكانيات الفضاء المعلوماتي و أن تسهم في ردع..... الإجرامية مع تطبيق الإجراءات..... المقررة في بيئة تكنولوجيا المعلومات.[2]

المبحث الأول : بيـــان مشكـــلات الحمايـــة الإجرائيـــة للمعلومـــات:

تعترض بالحماية الجنائية الإجرائية مشاكل عدة أبرزها صعوبة تحديد فاعل الجريمة و تقييم مدى و أثر الجريمة بالإضافة إلى مشاكل تتعلق بإتلاف البيانات الالكترونية (بالتعديل أو التغيير أو المحو) و التي هي موضوع للتنقيب الجنائي مما يعني تدمير أية أدلة من شأنها كشف الحقيقة أو التوصل إلى الجاني كما أن السرعة و السرية تعدان أهم العناصر الجوهرية في النجاح و التنقيب و التحري.[3]

مشكلات أخرى متعلقة بمدى كفالة قواعد الإجراءات التقليدية لحماية فاعلة لجرائم بيئة التجارة الالكترونية كإجراءات التفتيش و الضبط، التحفظ العاجل على البيانات[4] هذه المشاكل و غيرها نصت عليها اتفاقية بودابست 2001.

---

[1] - توصية 20.
[2] - بودابست 08.
[3] - دسوقي 496، بودابست 161.
[4] - دسوقي 496- 497.
تم توجيه دعوة للولايات المتحدة الأمريكية و اليابان و كندا و جنوب إفريقيا منذ توصية 1989/09 و توصية 1995/13 بصفة مراقب لتوسعة العضوية فيها و فتحها لغير الدول الأوربية و هو ما تقره المادة 38 من المشروع المعدل في 2000 و أيضا تكون الولايات المتحدة الأمريكية ذات مصلحة مباشرة بموضوع الجريمة عبر الانترنيت، دسوقي 491.

نشر المجلس الأوربي سنة 1989 دراسة أكد في توصياتها على ضرورة تفعيل دور القانون لمواجهة جرائم الحاسب الآلي أهم هذه التوصيات هي التوصية رقم 09 التي تبعتها دراسة أخرى عام 1995 حول الإجراءات الجنائية في مجال جرائم الانترنيت و التي تضمنتها التوصية 95/13، قام المجلس الأوربي (و المتكون من 41 دولة) سنة 1997 و على أساس التوصيتان السابقتان بتشكيل لجنة خبراء الجريمة عبر العالم الافتراضي *Committee of Experts on Crine in cyberspace* و ذلك لأجل إعداد اتفاقية في هذا المجال يحوي مضمونها و يتضمن ضرورة تسهيل التعاون الدولي في الإجراءات الخاصة بمتابعة الجرائم الناشئة عن الحاسوب و الانترنيت و صدر أول مشروع *Draft* لهذه الاتفاقية في شهر أفريل من عام 2000 بعنوان "**اتفاقية الجريمة عبر العالم الافتراضي**" ووافقت على المشروع 43 دولة أوربية أعضاء في المجلس الأوربي و مما سجل على هذا المشروع نقص في احتواء مجموعة جرائم كان يفترض أن تتضمنها بنود المشروع و نصوصه هذه الجرائم تعد في نظر المختصين في قانون الانترنيت يلزم النص عليها بنصوص جنائية و قد تضمنت هذه الاتفاقية ما يفيد اهتمام التشريعات المقارنة بموضوع الجريمة عبر الانترنيت و حاولت أن تؤسس لقواعد تعاون دولي في مجال المكافحة الدولية لمثل هذه الجرائم بنصها على ثلاث موضوعات أساسية:

أولا: مجموعة الجرائم التي يمكن أن تتركب بواسطة الحاسب الآلي و الانترنيت و من بينها جرائم التجارة الالكترونية.

ثانيا: مجموعة الإجراءات الجنائية التي يمكن اتخاذها في مواجهة هذه الجرائم.

ثالثا: موضوع التعاون الدولي بين الأعضاء الموقعين على هذه الاتفاقية.

أصدر الاتحاد الأوربي في أكتوبر 2000 مشروعا معدلا لهذه الاتفاقية ليكون من 48 مادة تتضمن عد لنصوص الموضوعية لمثل هذه الجرائم، حصر مجالات التعاون الدولي في إطار الإجراءات الجنائية.[1]

- في المواد 14 نطاق تطبيق نصوص قانون الإجراءات الجنائية.

---

[1] - دسوقي 489- 491.

- في المادة 16 التحفظ العاجل في البيانات المعلوماتية المخزنة.
- المادة 17 التحفظ و الإفشاء العاجل لبيانات المزور.
- المادة 19 تفتيش و ضبط البيانات المعالجة آليا المخزنة.
- المادة 21 اعتراض البيانات المتعلقة بالمحتوى.

بالإضافة إلى أحكام إجرائية أخرى متعلقة بسبل التعاون الدولي و قد وصف هذه المواد (من 14 إلى 21) خطوات إجرائية واجبة الأخذ بها على مستوى قومي بهدف التنقيبات الجنائية بالنسبة للجرائم المشار إليها في القسم الأول [1] و الجرائم الجنائية الأخرى عن طريق نظام معلوماتي و تجميع الأدلة المتعلقة بالجريمة الجنائية في شكل الكتروني.[2]

نشير إلى أن الاتفاقية تبنت وسائل إجرائية تقليدية كالتفتيش و الضبط في البيئة الرقمية كما أضافت عليها إجراءات أخرى جديدة مثل التحفظ العاجل على البيانات لإعطاء فعالية أكبر للإجراءات التقليدية لجمع البيانات و التفتيش و الضبط في بيئة تتميز بالتلاشي و سرعة اختفاء الأدلة.

و ما يمكن أن تشيره هذه الميزة في الدليل، و إن كان سبق التعرض لبعض هذه الإجراءات الجنائية المرتبطة بتكنولوجيا المعلومات.[3]

نصوص هذا القسم هدفت إلى السماح بالحصول أو جمع البيانات بهدف التنقيبات أو الإجراءات الجنائية التي تقود إليها و لم يستطع واصفوا الاتفاقية إدراج مسألة ما إذا كان يجب أن يفرض على مقدمي الخدمات الوسيطية الالتزام بالتجميع و الاحتفاظ ببيانات المرور خلال دورة محددة من الزمن لعدم اتفاق الأعضاء على

و فيما يلي نستقرء مضمون المواد الواردة في القسم الثاني من الاتفاقية:

---

[1] - و تعد الأحكام الموضوعية التي تضمنها القسم الأول من الاتفاقية جرائم متعلقة بصورة مباشرة مجال نشاط معاملات التجارة الالكترونية حيث تعلقت مواده بـ:

م 02 الولوج غير القانوني
م 03 الاعتراض غير القانوني
م 04 الاعتداء على سلامة البيانات
م 05 الاعتداء على سلامة النظام
م 06 إساءة استخدام أجهزة الحاسب
م 07 التزوير المعلوماتي
م 10 الجرائم المتصلة بالاعتداءات الواقعة على الملكية الفكرية في الحقوق المجاورة
م 11 الشروع و الاشتراك
م 12 مسؤولية الأشخاص المعنوية
م 13 الجزاءات و التدابير

[2] - هلالي، بودابست، 159

[3] - دسوقي 497، بودابست 162.

المـــادة [1]14:

أوجبت على كل طرف في الاتفاقية تبني إجراءات تشريعية ضرورية لأجل تشكيل سلطات و إجراءات بغرض التنقيبات و الإجراءات الجنائية المنصوص عليها و هذا القسم وفقا لقانونها الداخلي.

و تطبق السلطات و الإجراءات المشار إليها في الفقرة 1 على وجه لوجوب على :

- الجرائم الجنائية المنصوص عليها في المواد (2–11) من ذات الاتفاقية.
- كل الجرائم الجنائية الأخرى المرتكبة عن طريق نظام معلوماتي.
- جمع الأدلة الالكترونية بكل سرعة جنائية.

فيما عدا استثناء بنص المادة 21

كما أوجبت على الدول الأطراف النص في قانونهم الداخل على أن الأدلة في مثل هذه الجرائم يمكن أن تستخدم أمام القضاء في إطار الإجراءات الجنائية كيفما كانت طبيعة الجريمة الجنائية التي تكون موضوعا للمحاكمات الجنائية.

---

[1] **Article 14 : Portée d'application des mesures de droit de Procedure.**

1. Chaque Partie adopte les mesures législatives et autres que se révèlent nécessaires pour instaures les pouvoirs et procédures prévus dans la présente section aux fins d'enquête ou de procédures pénales spécifiques.
2. Sauf disposition contraire figurant à l'Article 21, chaque partie appliqué les pouvoirs et procédures mentionnés dans le paragraphe 1 :
   a. aux infractions pénales établies conformément aux articles 2-11 de la présente convention;
   b. à Toutes autres infractions pénales commises au moyen d'un système informatique ; et
   c. à la collecte des preuves électroniques de toute infraction pénale.
3. a. Chaque partie peut se réserver le droit de n'appliquer les mesures mentionnées à l'Article 20 qu'aux infraction ou catégories d'infractions spécifiées dans la réserve, pour autant que l'éventail de ces infractions ou catégories d'infractions ne soit pas plus réduit que celui des infractions auxquelles elle applique les mesures mentionnées à l'Article 21. Chaque partie envisagera de limiter une telle réserve de manière à permettre l'application la plus large possible de la mesure mentionnée à l'article 20.

   b. Lorsqu'une Partie, en raison des restrictions imposées par sa législation en vigueur au moment de l'adoption de la présente convention, n'est pas en mesure d'appliquer les mesures visées aux article 20 et 21 aux communications transmises dans un système informatique d'un fournisseur de services qui.

      i. est mis en œuvre pour le bénéfice d'un groupe d'utilisateurs fermé, et

      ii. n'emploi pas les réseaux publics de telecommunications et qui n'est pas connecté à un autre système informatique, qu'il soit public ou privé, cette partie peut réserver le droit de ne pas appliquer ces mesures à de telles communications. Chaque partie envisagera de limiter une telle réserve de manière à permettre l'application la plus large possible de la mesure mentionnée aux articles 20 et 21.

المـــادة 15[1]:و تعلقت بالشروط الضمانات

أوجبت هذه المادة على الأطراف فيها الحرص على تأسيس و تنفيذ و تطبيق السلطات و الإجراءات المنصوص عليها في هذا القسم في إطار ما لا يتعارض مع قانونها الداخلي و ما تكفل به حماية لحقوق الإنسان و حرياته المستمدة من الشرعة الدولية و التي يجب أن تتكافل مع مبدأ التناسب.

على أن تشمل وجوبا هذه الإجراءات على إشراف قضائي و حدود و بواعث و مبررات التطبيق كذا النظام التطبيق و مدته.

ثم تستدرج الاتفاقية بنودها في التعرض لموضوع التحفظ العاجل على البيانات المعلوماتية المخزنة في المادتين 16 و 17 اللتان تنطبقان على البيانات المخزنة التي تسبق تجميعها و الاحتفاظ بها عن طريق حائزي البيانات و لا تنطبق على التجميع في الوقت الفعلي.

المـــادة 16[2]:

---

[1] **Article 15 Conditions et sauvegardes:**

1. Chaque Partie Veille à ce que l'instauration, la mise en œuvre et l'application des pouvoirs et procédures prévus dans la présente section soient soumises aux conditions et sauvegardes prévues par son droit interne, qui doit assurer une protection adéquate des droits de l'homme et des libertés, en particulier des droits établis conformément aux obligations que celle-ci a souscrites en application de la convention de sauvegarde des droits de l'homme et des libertés fondamentales du conseil de l'Europe (1950) et du pacte international relatif aux droits civils et politiques de Nations Unies (1966) ou d'autres instruments internationaux applicables concernant les droits de l'homme, et qui doit intégrer le principe de la proportionnalité.
2. Lorsque cela est approprié eu égard à la nature de pouvoir ou de la procédure concerné, ces conditions et sauvegardes includent. Entre autres, une supervision judiciaire ou d'autres formes de supervision indépendante, des motifs justifiant l'application ainsi que la limitation du champ d'application et de la durée du pouvoir ou de la procédure en question.
3. Dans la mesure ou cela est conforme à l'intérêt public, en particulier à la bonne administration de justice, chaque Partie examine l'effet des pouvoirs et procédures dans cette section sur les droits, responsabilités et intérêts légitimes des tiers.

[2] **Article 16 : Conservation rapide de données informatiques Stockées.**

1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour permettre à ses autorités compétentes d'ordonner ou d'imposer d'une autre manière la conservation rapide de données électroniques spécifiés, y compris des données relatives au trafic, stockées au moyen d'un système informatique, notamment lorsqu'ily a des raisons de penser que celles-ci sont particulièrement susceptibles de perte ou de modification.
2. Lorsqu'une partie fait application du paragraphe 1 ci-dessus, au moyen d'une injonction ordonnant à une personne de conserver des données stockées spécifiés se trouvant en sa possession ou sous son contrôle, cette partie adopte les mesures législatives et autres qui se révèlent nécessaires pour obliger cette personne à conserver et protéger l'intégrité des données pendant une durée aussi longue que nécessaire, jusqu'à maximum 90 jours, afin de permettre aux

أوجبت على كل طرف أن يسن تشريعات أو يتخذ إجراءات يرى أنها ضرورية للسماح لسلطاته المختصة أن تفرض أو تأمر بالتحفظ على البيانات المعلوماتية المخزنة بواسطة نظام معلوماتي عندما تكون هناك أسباب تدعوا للاعتقاد بأن هذه البيانات معرضة للفقد أو التغيير، و تتخذ اتجاه ذلك كل الإجراءات التشريعية إلى تكوين ضرورية لأجل إجبار الشخص الذي في حوزته أو تحت إشرافه هذه البيانات على التحفظ على سلامتها لمدة طويلة من الزمن و حماية سلامة البيانات المذكورة بحد أقصاه 90 يوما لتمكين السلطات المختصة من الكشف عنها، كما يجب على كل طرف إجبار حارس البيانات على أن يحافظ على السرية في ما يتعلق بتطبيق الإجراءات.

المـــادة 17 [1]:

و عالجت هذه المادة مسألة التحفظ و الإفشاء العاجلان لبيانات المرور بأن أوجبت على كل طرف اتخاذ الإجراءات التشريعية أو أي إجراءات أخرى لضمان التحفظ على البيانات المتعلقة بالمرور لأجل:

- توفر التحفظ العاجل لهذه البيانات المتعلقة بالمرور بغض النظر عن وجود مزود خدمات واحد أو عدة مزودين ساهموا في نقل الاتصال.
- إبلاغ السلطة المختصة عن كمية بيانات مزود كافية لتحديد هوية مزودي الخدمات و طريق الاتصال الذي تم.
- و أوجبت خضوع سلطات و إجراءات هذه المادة للمادتين 14-15.

---

autorités compétentes d'obtenir leur divulgation. Une Partie peut prévoir qu'une telle injonction soit renouvelée par la suite.

3. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour obliger le gardien des données ou autre personne chargée de conserver celles-ci à garder le secret sur la mise en œuvre des procédures pendant la durée prévue par son droit interne.
4. Les pouvoirs et procédures mentionnés dans le présent article doivent être soumis aux articles 14 et 15.

[1] **Article 17 : Conservation et divulgation rapides de données relatives au trafic.**

1. Afin d'assuere la conservation des données relatives au trafic en application de l'articles 16, chaque Partie adopte les masures législatives et autres qui se révèlent nécessaires pour :
   a. Veiller à la conservation rapide de ces données relatives au trafic, qu'un seul ou plusieurs fournisseurs de services aient participé à la transmission de cette communication ; et
   b. Assuere la divulgation rapide à l'autorité compétent de la partie, ou à une personne désignée par cette autorie, d'une quantité de données relatives au trafic suffisante pour permettre l'identification des fournisseurs de service et de la voie par laquelle la communication a été transmise.
2. Les pouvoirs et procédures mentionnés dans le présent article doivent être soumis aux articles 14 et 15.

ثم تلت دلك مسألة الأمر بإنتاج بيانات معلوماتية تضمنتها المادة

المـــادة 18 [1]:

وجوب تبني تشريعات و إجراءات في إطار تأهيل سلطاته المختصة لأن تأمر:

- أي شخص يتواجد على إقليم تلك الدولة بإرسال بيانات في حوزته و المخزنة في نظام معلوماتي أو على دعامات تخزين.
- مقدم خدمات يشترط على إقليم تلك الدولة من أجل إرسال بيانات في حوزته متعلقة بالمشتركين و بتلك الخدمة.

و تتعلق هذه البيانات في هذه المادة بإمكانية تحديد:

- نوعية خدمة الاتصال و تقنياتها الفنية.
- الهوية، العنوان، رقم الهاتف، بيانات دفع الفاتورة و المبلغ المدفوع أي بيانات أخرى متوافرة على أساس عقد أو اتفاق تقديم الخدمة.

بعد ذلك استعرض هذا القسم إجراء تفتيش و ضبط البيانات المعلوماتية المخزنة.

المـــادة 19 [2]:

---

[1] **Article 18 : Injonction de produire.**

1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à ordonner :
   a. à une personne présente sur son territoire de communiquer les données informatiques spécifiées, en la possession où sous le contrôle de cette personne, et stockées dans un système informatique où un support de stockage informatique ; et
   b. à un fournisseur de services offrant des prestations sur le territoire de la partie, de communiquer les données en sa possession ou sous son contrôle relatives aux abonnés et concernant de tells services ;
2. Aux fins du présent article, l'expression ''données relatives au abonnés'' désigne toute information, contenue sous forme de données informatiques ou sous toute autre forme, détenue par un fournisseur de service et qui rapporte aux abonnées de ses services, autres que des données relatives au trafic ou au contenu, et permettant d'établir ;
   a. le type de service de communication utilisé, les dispositions techniques prises à cet égard et la période de service ;
   b. l'identité, l'adresse postale ou géographique et le numéro de téléphone de l'abonné, et tout autre numéro d'accès, les données concernant la facturation, et le paiement disponibles sur la base d'un contrat ou d'un arrangement de service ; (available on the basis of the service agreement or arrangement)
   c. toute autre information relative à l'endroit où se trouvent les équipements de communication diponible sur la base d'un contrat ou d'un arrangement de service.

[2] **Article 19 : Perquisition et saisie de données informatiques stockées.**

1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à perquisitionner ou à accéder d'une façon similaire :
   a. à un système informatique ou à une partie de celui-ci ainsi qu'au données informatique qui y sont stockées ; et
   b. à un support du stockage informatique permettant de stocker des données informatique sur son territoire.

أوجبت هذه المادة على كل طرف من تشريعات تخول لسلطاته المختصة سلطة التفتيش أو الولوج بطريقة متشابهة أي: (فقرة 1)

- لكل نظام معلوماتي أو لجزء منه و كذلك للبيانات المعلوماتية المخزنة فيه و على إقليمه.
- دعامة تخزين عليها بيانات معلوماتية.

مع وجوب أسباب تدعوا للاعتقاد بأن البيانات التي تسعى إليها مخزنة في هذا النظام أو هي موجودة على هذه الدعامة أو في جزء من النظام (فقرة 2) ضرورة سن تشريعات تخول سلطاته المختصة سلطة ضبط أو الحصول على البيانات، هذه الإجراءات تشمل السلطات التالية حسب الفقرة 3:

- ضبط أو الوصول بطريقة متشابهة إلى نظام معلوماتي أو جزء منه أو إلى دعامة تخزين.
- التحقق و التحفظ على نسخة من هذه البيانات.
- المحافظة على سلامة البيانات المخزنة.
- منع حذف هذه البيانات من النظام.

كما يجب على الدول الأطراف حسب الفقرة 4 أن تخول سلطاتها المختصة صلاحية إصدار الأمر لأي شخص لديه معلومات عن تشغيل النظام لأجل حماية البيانات المعلوماتية التي تضمن تقديم كل المعلومات الضرورية على نحو معقول يسمح بتطبيق الإجراءات السابقة للإشارة إليها.

---

2. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour veiller à ce que, lorsque ses autorités perpuisitionnent ou accèdent d'une façon similaire à un système informatique spécifique ou à un partie de celui-ci, conformément au paragraphe 1 (a), et ont des raisons de penser que les données recherchées sont stockées dans un autre système initial ou disponibles ce système initial, lesdites autorités soient en mesure d'étendre rapidement la perquisition ou un d'un accès d'une façon similaire à l'autre système.
3. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à saisir ou a obtenir d'une façon similaire les données informatiques pour lesquelles l'accès a été réalisé en application des paragraphes 1 ou 2. Ces mesures incluent les prérogatives suivantes :
    a. saisir ou obtenir d'une façon similaire un système informatique ou une partie de celui-ci ou un support de stockage informatique :
    b. réaliser et conserver une copie des ces données informatiques :
    c. préserver l'intégrité des données informatiques stockées pertinentes ; et
    d. render inaccessibles ou enlever ces données informatiques du système informatique consulté.
4. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à ordonner à toute personne connaissant le fonctionnement du système informatique ou les mesures appliqués pour protéger les données informatiques qu'il contient de fournir toutes les informations raisonnablement nécessaires, pour permettre l'application des mesures visées par les paragraphes 1 et 2.
5. Les pouvoirs et procédures mentionnés dans cet article doivent être soumis aux articles 14 et 15.

كما تضمنت الاتفاقية النص على إجراء التجميع في الوقت الفعلي للبيانات المعلوماتية حيث تعلق نص **المـــادة 20** [1]بالتجميع في الوقت الفعلي للبيانات الخاصة بالمرور حيث نصت على وجوب تخويل السلطات القضائية بواسطة إجراءات تشريعية أو أية تشريعات أخرى تكون ضرورية (في الفقرة 01) و منحها صلاحيات متعلقة بـــ:

- جمع أو تسجيل معلومات بوسائل فنية موجودة على إقليمه.
- إجبار مزود الخدمات – حسب قدرته الفنية – أن يجمع أو يسجل بواسطة وسائل فنية موجودة على إقليمه.
- و أن يقدم كل العون و المساعدة للسلطة المختصة من أجل تجميع أو تسجيل في الوقت الفعلي البيانات المتعلقة بالمرور.

و في الفقرة 3 من ذات المادة أوجبت إلزام مقدم الخدمات على المحافظة على سرية أي معلومات متعلقة بهذا الشأن أو أسرار الواقعة الخاصة بممارسة ما سبق النص عليه من سلطات في هذه المادة.

أما **المـــادة 21** [2]فقد تعلقت بمسألة مهمة و هي اعتراض البيانات الخاصة بالمحتوى حيث ورد في هذه المادة وجوب منح و تخويل السلطات المختصة المكنات في ما يتعلق بالجرائم الخطيرة

---

[1] **Article 20 : Collecte en temps réel des données relatives au trafic.**

1. Chaque Partie adoptes mesures législatives et autres qui se révèlent nécessaires pour habiliter des autorités compétentes à :
   a. Collecter ou enregistrer par l'application de moyens techniques existant sur son territorire :
   b. Obliger un fournisseur de services, dans le cadre de ses capacités technique existantes, à :
      i. Collecter ou enregistrer par l'application de moyens technique existant sur son territoire, ou
      ii. Prêtre aux autorités compétentes son concours et son assistance pour collecter ou enregistrer, en temps réel, les données relatives au trafic associées à des communications spécifiques transmises sur son territoire au moyen d'un système informatique.
2. Lorsqu'une Partie, en raison des principes établis de son ordre juridique interne, ne peut adopter les mesures énoncées au paragraphe (a), elle peut à la place, adopter les mesures législatives et autres qui se révèlent nécessaires pour assurer la collecte ou l'enregistrement en temps réel des données relatives au trafic associées à des communications spécifiques transmises sur son territoire par l'applications de moyens technique existant sur ce territoire.
3. Chaque Partie adoptes mesures législatives et autres qui se révèlent nécessaires pour obliger un fournisseur de services à garder secrets le fait que l'un quelconque des pouvoirs prévus dans le présent article a été exécuté, ainsi que toute information à ce sujet.

[2] **Article 21 : Interception de données relatives au contenu.**

1. Chaque Partie adoptes mesures législatives et autres qui se révèlent nécessaires pour habiliter des autorités compétences relativement à un éventail d'infractions graves à définir en droit interne, à :
   a. Collecter ou enregistrer par l'application de moyens techniques existant sur son territoire ; et
   b. Obliger un fournisseur de services, dans le cadre de ses capacités technique existantes, à :
      i. Collecter ou enregistrer par l'application de moyens technique existant sur son territoire, ou

التي يحددها القانون الداخلي وفق ما يلي: الجمع و التسجيل و إلزام مزود الخدمات على التعاون في ذلك بوسائل فنية موجودة على إقليم و تبني كل الإجراءات التشريعية لتسهيل ذلك.

المبحث الثاني : دور التعـــاون الدولي فـــي مواجهـــة جرائـــم التجـــارة الالكترونيـــة

بحكم أن طبيعة المعاملات التجارية الالكترونية غير متقيدة بحدود إقليمية لدولة بعينها فإن هذه الطبيعة منعكسة بالضرورة على التجارة الالكترونية حيث تمتاز هذه الجرائم بكونها جرائم عابرة للحدود و هو ما يجعل من الضرورة الواقعية إعمال مبدأ التعاون الدولي لأجل مكافحة و التصدي لهذه الجرائم ذات الطبيعة الالكترونية المتخطى للحدود الإقليمية لدول، و إذا تحقق فعلا وجود البعد الدولي في جرائم المعلوماتية عموما و جرائم التجارة الالكترونية على وجه الخصوص باعتبارها جرائم عابرة للحدود إلا أن هذا البعد لم يرشحها إلى درجة اعتبارها جرائم دولية يتولى القانون الدولي الجنائي تنظيمها و النص عليها في إطار اختصاص محاكم جنائية دولية فالبعد الدولي الذي تكتسبه جرائم التجارة الدولية المعروفة، فبعضها متصل بالجرائم العالمية التي هي من قبيل الجرائم الداخلية ذات العالمي و التي تعاقب عليها التشريعات الوطنية الداخلية و هو ما يدعوا إلى تحقيق تعاون دولي فعال يسعى ابتداء و بدرجة أولى إلى تقليص الفوارق بين الأنظمة العقابية و توحيد ما أمكن من إجراءات قد تؤدي إلى و بدرجة أولى إلى تقليص الفوارق بين الأنظمة العقابية و توحيد ما أمكن من إجراءات قد تؤدي إلى تضييق و الحد من الظاهرة الإجرامية.[1]

---

ii. Prêtre aux autorités compétentes son concours et son assistance pour collecter ou enregistrer, en temps réel, les données relatives au trafic associées à des communications spécifiques transmises sur son territoire au moyen d'un système informatique.

2. Lorsqu'une Partie, en raison des principes établis de son ordre juridique interne, ne peut adopter les mesures énoncées au paragraphe (a), elle peut à la place, adopter les mesures législatives et autres qui se révèlent nécessaires pour assurer la collecte ou l'enregistrement en temps réel des données relatives au trafic associées à des communications spécifiques transmises sur son territoire par l'applications de moyens technique existant sur ce territoire.
3. Chaque Partie adoptes mesures législatives et autres qui se révèlent nécessaires pour obliger un fournisseur de services à garder secrets le fait que l'un quelconque des pouvoirs prévus dans le présent article a été exécuté, ainsi que toute information à ce sujet.

[1] - محمود عبابنة، جرائم الحاسوب، ص 118.

و إذا كان هذا التعاون الدولي آلية فعالة للتصدي لهذه الجرائم فإن هذا التعاون يقتضي التخفيف من تلك الفوارق بين الأنظمة العقابية الداخلية و السير في اتجاه التقريب بين هذه القوانين الجنائية الوطنية لأجل محاصرة و تضييق الثغرات التي يتحلل بواسطتها مجرمو هذه المعاملات[1] – فما هو أمر مخالف لنصوص قوانين داخل دولة ما هو أمر غير مجرم لدى دولة أخرى مما يجعل أصحاب تلك المؤسسة يبحثون عن أوفق النظم لمعاملاتهم فيؤسسون بها فروعا تجارية،[2] و بالمقابل فإن غياب هذا التعاون يزيد من هذه الجرائم عموما العابرة للحدود و الجرائم الالكترونية بدرجة خاصة.[3]

أ– **و يخص البعض مبررات** لهذا التعاون الدولي في مكافحة هذه الجريمة، هذه المبررات أهمها:[4]

- يعتبر خطوة لأجل تدويل قواعد جنائية في سبيل خلق قانون جنائي دولي لأجل مكافحة الجريمة المنظمة و العابرة للحدود.
- أنه يعد من التدابير الوقائية التي تحول دون وقوع و ارتكاب هذه الجرائم حيث من شأن تعميم العقوبة أو ورودها في أكثر تشريعات الدول أن يحد من النشاط الإجرامي بوجود موانع عقابية أينما مارس النشاط، هو الأمر الذي يحقق ردعا للمجرم الالكتروني، و يقلل من نسبة الظاهرة الإجرامية.
- الاستفادة من خبرة كل طرف في مواجهة هذه الجرائم و تعميم النافع فيها.
- يظهر في الجانب الآخر وجود تنسيق قوي و تنظيم مهيكل بين أقطاب الإجرام و تبادل للمعلومات حتى أن لهؤلاء مؤتمرات سنوية تعقد في إطار تعزيز آليات العمل،[5] فهل يمكن لتنظيمات عالمية كهذه مواجهتها دون تنسيق أو تعاون دولي.
- أثر هذه الجرائم لا يقتصر على الجانب الوطني أو الإقليمي بل يمتد إلى النطاق الدولي و العالمي[6] وجود تحولات على هذه الظاهرة الإجرامية متمثلة في انتقالها من ظاهرة فردية

---

[1] **Christophe CARON, Vers un droit pénal communautaire de la contrefaçon,** Revue **Communication Commerce électronique n° 6, Juin 2007, Repère 6**

[2] - تقيم المؤسسات الاستشارة و الخدمات الالكترونية الأمريكية فقراتها خارج إقليم الولايات المتحدة الأمريكية تهربا من النظم الطابعة لهذه الدولة و بحثا عن نظم أوفق لها، بالإضافة إلى الحفاظ تكلفة مشاريعها ورخص العمالة و وجدت في الدول الآسيوية ملاذا خالصا و لعل الهند أكثر الدول استقبالا لهذه المؤسسات.

[3] - دسوقس، ص 591.

[4] - دسوقي، ص 592.

[5] - عقد مؤتمر سنوي لمجرمي المعلوماتية ناقشو فيه أخلاقيات مهنة القرصنة، يرجع إلى الحجازي، الحماية الجنائية.

[6] - عبابنة، ص 120.

لأمن النظم و المعلومات و شبكات الاتصال إلى ظاهرة عامة شكلت أخطر أشكال الإجرام المنظم.[1]

ب- أمـــام هذه المبـــررات و غيرها ندرك أن التعاون دولي هو حتمية عاجلة للوقاية من هذه الجرائم و الدول فرادى أعجز من أن تستطيع أن تتصدى لها دون التنسيق و تعاون جهات إقليمية و دولية معها لكن أمام هذا التعاون بعض الصعوبات التي ينبغي التفكير جديا للتغلب عليها و حلها فيها:[2]

- أن بعض التشريعات الجنائية التقليدية تحول دون فعالية التعاون الدولي إن وجد.
- اختلاف التشريعات الجنائية الوطنية حول مضمون الأفعال (الركن الشرعي) المجرمة هو في ذاته عقبة دون تحقيق التعاون أهدافه.
- كون التمايز الحضاري – درجة الاعتماد على التبعية و ممارستها و ارتكاز المعاملات التجارية عليها – يشكل أقوى الفوارق، و كذلك التمايز التشريعي الذي هو محصلة الاندماج في المنظومة الرقمية يترتب عليه مشاكل متعلقة بالطبيعة الخاصة، العقوبات، الاختصاص، الإجراءات و الإثبات.

و لعل أهم المواضيع التي يمكن أن يرتكز عليها موضوع التعاون الدولي هي:[3]

- حل مشكلات الاختصاص القانوني و القضائي باتخاذ التدابير الملائمة فيما يمكن أن تشيره جرائم التجارة الالكترونية عابرة للحدود.
- تنظيم إجراءات التفتيش و ضبط المعلومات دون الاعتداد على حقوق الأفراد و حرياتهم أو سيادة الدول.
- تطوير أدلة الإثبات و إعادة النظر في مدى حجية المستندات الالكترونية في الإثبات طبقا لما استحدث من آليات تعامل بين الأفراد و بالأخص المعاملات التجارية الالكترونية (المستند الالكتروني – السجل الالكتروني...).
- تسليم المجرمين و المسائلة القضائية فيما يتعلق بمسائل الجرائم الالكترونية

و قد كان هذا التعاون موضوع مدارسة و اهتمام على مستوى إقليمي فقد كان من بين أهم أعمال المجلس الأوربي في هذا المجال هو إشرافه على اتفاقية بودابست الموقعة في 23 نوفمبر

---

[1] - عبابنة الرزاقي، ص 119.
[2] - عبابنة الرزاقي، ص 120- 121.
[3] - دسوقي، ص 616.

2001 حيث دعى في المذكرة التفسيرية لهذه الاتفاقية الدعوة إلى أن يواكب القانون الجنائي التطورات التكنولوجية، و أن يعمل على ردع الأفعال الإجرامية و خصصت الاتفاقية الباب الثالث من أصل أربعة أبواب مسألة التعاون الدولي و اشتمل هذا الباب على قسمين:

الأول: المبادئ العامة

الثاني: الأحكام الخاصة[1]

و اتفاقية بودابست قد خصصت لهذا الأمر مجموعة نصوص من اتفاقياتها و ذلك فيما تعلق التعاون الدولي في مكافحة جرائم المعلوماتية العابرة للحدود فعالجت هذه الاتفاقية مواضيع:

- الأحكام العامة المتعلقة بالتعاون الدولي.
- تسليم المجرمين.
- المساعدة القضائية المتبادلة.

و سنتناول أهم النصوص التشريعية التي وردت في هذا الفصل من الاتفاقية:

المطلب الأول : الأحكـــام العامـــة المتعلقـــة بالتعـــاون الدولـــي

نصت هذه الأحكام المادة 23 [2]فيها حيث أوجبت على الأطراف أن تتعاون مع بعضها البعض بتطبيق الأصول الدولية المتصلة بالتعاون الدولي في المواد الجنائية إلى أوسع نطاق لأغراض التنقيب و التحري أو الإجراءات الجنائية المتعلقة بالجرائم الجنائية المرتبطة بنظم و بيانات معلوماتية أو جمع أدلة ذات شكل الكتروني للجريمة الجنائية.

---

[1] - محمود مسعود محمد خليفة، ص 74.

[2] **Article 23 : Principes généraux relatifs à la coopération internationale.**

Les parties coopèrent conformément aux dispositions du présent chapitre, en application des instruments internationaux pertinents sur la coopération internationale en matière pénale, des arrangements reposant sur des législations uniformes ou réciproques et de leur droit national, dans la mesure la plus large possible les unes avec les autres, aux fins d'investigations ou de procédures concernant les infractions pénales liées des systèmes et données informatiques ou pour recueillir les preuves sous forme électronique d'une infraction pénale.

و الملاحظ على هذا التعاون الواجب إعماله هو التزام مفروض على الأطراف و بصفة موسعة مما يوجب تذليل الصعوبات في سبيل تبادل المعلومات و الأدلة، مع وجوب مد نطاق هذا التعاون ليشمل كل الجرائم الجنائية المرتبطة بنظم و بيانات معلوماتية [1] و هي تلك الجرائم التي تطرقنا فيما سبق و الواردة في ذات الاتفاقية و المتعلقة بـــ الولوج غير القانوني (المادة 2)، الاعتراض غير القانوني (المادة 3)، الاعتداء على سلامة البيانات (المادة 4)، الاعتداء على سلامة النظام (المادة 5)، إساءة استخدام أجهزة الحاسب أو معداته (المادة 6)، التزوير المعلوماتي (المادة 7)، الغش المعلوماتي (المادة 8)، الجرائم المتصلة بالمواد الإباحية للطفولة (المادة 9)، الجرائم المتصلة بالاعتداءات الواقعة على الملكية الفكرية و الحقوق المجاورة (المادة 10)، المشروع و الاشتراك (المادة 11) ثم بالإضافة إلى تجميع الأدلة ذات شكل الكتروني للجريمة.

المطلب الثاني : تسليـــم المجرميـــن:

تضمنت نصوص هذه الاتفاقية النص على هذا الإجراء و ذلك ضمن نص المادة 24[2] و نشير إلى أن هذه الاتفاقية قد عينت بهذا الإجراء حماية فائقة لما تضمنه هذا النص من أحكام حيث جاءت الفقرة الأولى منها مقسمة إلى بندين:

---

[1] **Agathe LEPAGE, Réflexions de droit pénal sur la loi du 6 août 2004 relative à la protection des personnes à l'égard des traitements de données à caractère personnel, Revue Droit pénal n° 3, Mars 2005, Etude 5**

[2] **Article 24 : Extradition**

1. a. Le présent article s'applique à l'extradition entres les Parties pour les infractions pénales définies conformément aux articles 2 à 11 de la présente Convention, à condition qu'elles soient punissables dans la législation des deux Parties concernées par une peine privative de liberté pour une période maximale d'au moins un an, ou par une peine plus sévère.
   b. Lorsqu'il est exigé une peine minimale différente, sur la base d'un traité d'extradition tel qu'applicable entre deux ou plusieurs parties, y compris la Convention européenne d'extradition (STE n° 24), ou d'un arrangement reposant sur des législations uniformes ou réciproques, c'est la peine minimum prévue par ce traité ou ce arrangement qui s'applique.

2. Les infractions pénales décrites au paragraphe 1 du présent article sont considérées comme incluses en tant qu'infractions pouvant donner lieu à extradition dans tout traité d'extradition existant entre ou parmi les Parties. Les Parties s'engagent à inclure de telles infractions comme infractions pouvant donner lieu à extradition dans tout traité d'extradition pouvant être conclu entre ou parmi elles.
3. Lorsqu'une de Partie conditionne l'extradition à l'existence d'un traité et reçoit une demande d'extradition d'une autre Partie avec laquelle elle n'a pas conclu de traité d'extradition, elle peut considérer la présente Convention comme fondement juridique pour l'extradition au regard de toute infraction pénale mentionnée au paragraphe 1 du présent article.

أتت الفقرة أ مجال انطباق أحكام تسليم المجرمين بين الأطراف حيث حصرتها في الجرائم الجنائية، الواردة في المواد من 2- 11 من ذات الاتفاقية و اشترطت لذلك أن يكون معاقبا عليها في تشريع الطرفين بعقوبة سالبة للحرية لا تقل عن سنة أو بعقوبة.....

و تطبيق العقوبة المنصوص عليها في هذه الاتفاقية في حالة كان الأمر يتطلب تطبيق عقوبة دنيا مختلفة على أساس اتفاق سابق و هذا فحوى البند الثاني من الفقرة الأولى.

كما أوجبت الفقرة الثانية اعتماد الجرائم المنصوص عليها في هذه المادة (م 2- 11 من ذات الاتفاقية) جرائم تستوجب تسليم المجرمين في كل اتفاق يتم بين الأطراف و تدمج هذه الجرائم على وجه الإلزام بوصفها جرائم تستوجب تسليم المجرمين في كل اتفاق يعقد بينهم أو من خلالهم لتسليم المجرمين.

كما أمكن اعتبار هذه الاتفاقية أساسا قانونيا لتسليم المجرمين (بالنسبة لكل جريمة مشار إليها في الفقرة الأولى في ذات المادة في حالة اشتراط أحد الأطراف أن يكون تسليم المجرمين متوقفا على وجود اتفاق سابق لتلقي طلب التسليم من طرف آخر غير مرتبط معه باتفاقية تسليم و هذا ما أوردته الفقرة 3، كما أن إجراء التسليم يخضع للشروط المنصوص عليها بواسطة القانون الداخلي للطرف المطلوب منه التسليم أو لاتفاقيات تسلم المجرمين (فقرة 5) و في حالة رفض تسليم المجرم، بالنسبة لجريمة مشار إليها في الفقرة الأولى من ذات المادة بناء على جنسيته

---

4. Les Partie qui ne conditionnent pas l'extradition à l'existence d'un traité reconnaissent les infractions pénales mentionnées au paragraphe 1 du présent article comme des infractions pouvant donner lieu entre elles à l'extradition.
5. L'extradition est soumise aux conditions prévues par le droit interne de la Partie requise ou par les traités d'extradition en vigueur, y compris les motifs pour lesquels la Partie requise peut refuser l'extradition.
6. Si l'extradition pour une infraction pénale mentionnée au paragraphe 1 du présent article est refusée uniquement sur la base de la nationalité de la personne recherchée ou parce que la Partie requise s'estime compétent pour cette infraction, la Partie requise soument l'affaire, à la demande de la Partie requérante, à ses autorités compétentes aux fins de poursuites, et rendra compte en temps utile de l'issue de l'affaire à la Partie requérante. Les autorités en question prendront leur décision et mèneront l'enquête et la procédure de la même manière que pour toute autre infraction de nature comparable conformément à la législation de cette Partie.
7. a. Chaque Partie communiqué au Secrétaire générale su Conseil de l'Europe, au moment de la signature ou de dépôt de son instrument de ratification, d'acceptation, d'approbation ou d'adhésion, le nom et l'adresse de chaque autorité responsable de l'envoi ou de la réception d'une demande d'extradition ou d'arrestation provisoire, en l'absence de traité.

b. Le Secrétaire général du Conseil de l'Europe établit et tient à jour un registre des autorités ainsi désignées par les Partie. Chaque Partie doit veiller en permanence à l'exactitude des données figurant dans le registre.

المطلوب أو لكون الطرف المطلوب منه لتسليم يرى بأنه مختص بهذه الجريمة فإن الطرف المطلوب منه التسليم..... إلى سلطاته المختصة بهدف التحقيقات بناء على طلب الطرف الملتمس.[1]

المطلب الثالث : المساعـــدة القضائيـــة

في إطار تعاون دولي فعال يمد من الظاهرة الإجرامية المتنامية من جهة المتناسقة بين أقطابها فإنه و لأجل و لأجل تحقيق الهدف من التعاون الدولي الذي هو الآن أصبح أكثر من ضرورة فإنه يتوجب على الأطراف أن ترفع من حد التنسيق بينها و تمد العون لبعضها البعض على غرار تلك الإجراءات التي تضمنتها اتفاقية بودابست في إطار التحقيقات باقي الجرائم الجنائية المرتبطة منظم بيانات معلوماتية أو بغرض جمع الأدلة الالكترونية للجريمة، وأوجبت الاتفاقية في المادة 25[2] فيها على كل طرف تبني إجراءات تشريعية لأجل الوفاء بالالتزامات المنصوص عليها فيما يلي من المواد (27– 35) كما أمكنت لأي طرف في حالة الاستعجال أن يقدم طلبا للمساعدة المتبادلة أو الاتصالات عن طريق وسائل مستحدثة و أوجبت على الدولة المقدم إليها الطلب أن توافق و أن ترد على الطلب المقدم إليها بأي وسيلة عاجلة.

---

[1] - و تؤسس الدول المنظمة إلى الاتفاقية الأوربية للتعاون رفضها تسليم المجرمين على كون أن من شأنه التسليم في جرائم معينة مساس بمصالحها القومية فبعض الجرائم يمكن أن يمس بمصالح حيوية و أساسية للدولة و ذلك في حالة الدخول مثلا إلى قواعد بيانات إستراتيجية متعلقة بقطاعات مالية أو اقتصادية.

[2] **Article 25 : L'entraide judiciaries:**

1. Les Parties s'accordent l'entraide la plus large possible aux fins d'investigations ou de procédures concernant les infractions pénales liées à des systèmes et des données informatiques ou afin de recueillir les preuves sous forme électronique d'une infraction pénale.
2. Chaque Partie adopte également les mesures législatives et autres qui se révèlent nécessaires pour s'acquitter des obligations énoncées aux articles 27 à 35.
3. Chaque Partie peut, en cas d'urgence, formuler une demande d'entraide ou les communications s'y rapportant par des moyens rapides de communication, tels que la télécopie ou le courrier électronique, pour autant ces moyens offrent des conditions suffisantes de sécurité et d'authentification (y compris le cryptage si nécessaire), avec confirmation officielle ultérieure si l'Etat requis l'exige. L'Etat requis accepte la demande et y répond par n'importe lequel de ces moyens rapides de communication.
4. Sauf disposition contraire expressément prévue dans les articles du présent Chapitre, l'entraide est soumis aux conditions fixées par le droit interne de la Partie requise ou par les traités d'entraide applicables, y compris les motifs sur la base desquels la Partie requise peut refuser la coopération. La Partie requise ne doit pas exercer son droit de refuser l'entraide concernant les infractions visées aux articles 2 à 11 au seul motif que la demande porte sur une infraction qu'elle considère comme de nature fiscale.
5. Lorsque, conformément aux dispositions du présent chapitre, la Partie requise est autorisée à subordonner l'entraide à l'existence d'une double incrimination, cette condition sera considérée comme satisfaite si le comportement constituant l'infraction, en relation avec laquelle l'entraide est requise, est qualifié d'infraction pénale par son droit interne, que le droit interne classe ou non l'infraction dans la même catégorie d'infractions ou qu'il la désigne ou non par la même terminologie que le droit de la Partie requérante.

مع العلم أن هذه المساعدة تخضع لشروط المحددة في القانون الداخلي للطرف الموجه له الطلب أو عن طريق الاتفاقات المطبقة و قد عززت هذه الاتفاقية أسلوب التعاون بين أطرافها بفعل ما أقرته من أسلوب المعلومات التلقائية و بالضبط في المادة 26 أن يرسل لأي طرف آخر معلومات تحصل عليها في نطاق تقنياته الخاصة به إذا ما قدر أن هذه المعلومات تساعد الطرف المرسل إليه في الإسهام في إجراءات تنقيب أو تحقيق متعلق بجرائم متضمنة بذات الاتفاقية، عندما تكون هذه الجرائم يمكن أن تؤدي إلى طلب المساعدة بواسطة هذا الطرف مع قيام إمكانية اشتراط الطرف المرسل الاحتفاظ بسرية المعلومات أو استخدامها وفقا لشروط معينة مع وجوب تقييد الطرف المرسل إليه المعلومات بهذه الاشتراطات إن وجدت، و إعلام الطرف المرسل بمدى مقدرته على ذلك.

الخاتمـــــــــة:

الحكم عن الشيء فرع عن تصور و هذا ما جعلنا نبحث ماهية المعاملات التجارية الالكترونية، و هل هناك من فوارق من هذه المعاملات التقنية المستحدثة و بين الأنشطة التجارية التقليدية فوجدنا أنه ليس هناك فوارق تجعل المعاملان تختلفان عدا ما يمكن يفرق بينهما من حيث آلية التواصل بين أطراف العلاقة التعاقدية التجارية (التعاقد عن بعد).

أما عن الآثار التي تحدثها هذه المعاملات فهي ذات الآثار القانونية التقليدية إلا أن حجم التعامل بها ضاعف من نسبة الأرباح و تقليص المسافات و اختصار الزمن و في المقابل هذه الإيجابيات استحدث ذلك النمط الحديث من الجريمة فبقدر ما وفرت التجارة الالكترونية من فرص للتبادل الحر للسلع و الخدمات و المنافع فتحت باب مضار أصبح يهدد مصالح محمية و مراكز قانونية قائمة ما استدعى الإسراع في تشريع قوانين من شأنها كفالة حماية جنائية ضد هذا النوع المستحدث من الجرائم أو على الأقل تعديل تلك القواعد القائمة لتمثيل حمايتها و تأمن ذلك التهديد الذي تهدد به هذه الجرائم لمعاملات التجارة الالكترونية و في هذا الإطار رأينا أن القواعد القانونية القائمة التقليدية يمكن أن نحكم بعدم كفاية أطرها العقابية لكفالة حماية جنائية حقه لمعاملات التجارة الالكترونية (.....).

أو ما تعلق بكفالة الحماية الجنائية لمضمون النشاط بحد ذاته (.....) و على ذكر مضمون النشاط ينبغي التأكيد على دعوة الأخذ جديا باعتبار الكيانات المعنوية حقوقا تفرد لها حقوقا تفرد لها الحماية، و نخص بالتأكيد اعتبار المال المعلوماتي مالا منقولا، تطاله أحكام السرقة و باقي الأحكام من نصب و احتيال و خيانة للأمانة

ثم إن معاملات التجارة الالكترونية تفرض على المشرع (في حالة اعتماده هذه الآلية فعلى المستوى الوطني (الجزائر) و تزال هذه الآلية ضعيفة الاعتماد نسبيا) أن ستفرغ جهده في حماية أطراف العلاقة التعاقدية بالأخص الطرف الأضعف فيها ألا و هو المستهلك حيث لا يمكن إقامة توازن فعلي و حقيقي من طرفي معاملات التجارة

الالكترونية فلا يزال الطرف الحرفي متمكنا من آلياتها و فنياتها الإعلانية و التسويقية بما يملك من قدرات و مؤهلات و تتعاظم معها رغبته في تحقيق الربح و المنفعة مما يجعل المستهلك في مركز أضعف حيث أصل العقود المشاعة .

نذكر بأنه كما رأينا أنه من خلال هذه الحماية التي ينبغي تقريرها نجد من دوافع تقريرها هو حماية ذلك الحق الدستوري ضد أي اعتداء يهدده أو يقع عليه و هذا أمر لا يثير إشكالات جمة حال تقرير الحماية الجنائية له، لكن ما يدعوا إلى تأكيده هو وجوب إحداث توازن عملي و فعلي من جانب الأحكام الموضوعية المتعلقة بالحماية الجنائية للتجارة الالكترونية لكن الأمر يستدعي الدعوة إلى إحداث توازن عملي و فعلي حينما يتعلق بالأحكام الإجرائية لذات الحماية حيث يمكن أن ينتزع بدعوى حماية الحقوق و إجراءات المتابعة أو التحقيق لنجد تهديدا ملموسا لكثير من الحقوق..... بحيث هذا الحق يقع انتهاكه تحت طائلة القانون، و لعلنا نجد في المشرع الفرنسي نموذجا كاد يكون متحيزا للحق في الخصوصية في إطار تقرير الحماية الجنائية للمعاملات الالكترونية و هذا أمر مستساغ لتلازم هذا الحق بالحقوق الإنسانية فهو حق منصوص عليه في كل الدساتير و مقر في الشرائع الدولية، و بخلاف ذلك انتهج المشرع الأمريكي بحجية الحرب على الإرهاب و حماية الأمن القومي نهجا آخر بهذا الحق و اعتدى عليه و بالأخص في القواعد الإجرائية الضابطة للتفتيش و هذا ما لا ندعو للاقتداء به أو الحذو حذوه.

كما رأينا أن التجارة الالكترونية على خلاف معاملات النشاط التجاري التقليدي فإن آثار معاملاتها تمتد إلى غير أطراف العلاقة التعاقدية التجارية و هذا ما دعانا إلى التطرق إلى دور وسطاء خدمة الإنترنيت في هذه المعاملة و مدى المسؤولية الملقاة عليه.....

و هو ما استدعى التأكيد على ضرورة إلزام هؤلاء الوسطاء على التعاون مع الجهات القضائية في حدود ما يسمح به القانون و عدم الإضرار بحقوق محمية.

إنه و لكسب ثقة المتعاملين بآليات التجارة الالكترونية و ضمان نمائها وجب تعزيز الحماية للجنائية للتوقيع الالكتروني، أولا بإقراره و الدعوة إلى شيوع التعامل به

و الاعتراف بحجيته في إطار المعاملات التجارية على الأقل اعتماد نوع يمكن أن تتوفر فيه عوامل أو شروط عملية حمائية.

ثم حماية ضد ما يمكن أن يقع عليه من تزوير الذي لا يطاله وحده بل يمكن أن يمتد هذا الفعل الجرمي إلى باقي المحررات و المستندات الالكترونية التي تدخل في إطار المعاملات التجارية الالكترونية.

ثم إن هذه المعاملات الالكترونية و إن سهلت أساليب النشاط التجاري بالنسبة لأطراف علاقاتها التعاقدية فإنها كذلك سهلت عليهم فكرة التهرب من سداد المستحقات الضريبية، لذلك وجدنا أن أنجع وسيلة لمكافحة أو التصدي لهذه الجريمة هي وجوب تعاون الوسطاء الماليين (بنك...) و وسطاء الخدمة (مورد خدمات، مزود الخدمة...) مع الجهات الضريبية للإفادة بالتحويلات المالية و بيانات الأعمال لأجل رصد المعاملات التجارية، و وجدنا أن اقتراح الاقتطاع العضوي آلية من شأنها أن تخفض من نسبة التهرب الضريبي و تصد هذه الجريمة، حيث يعد ذلك الاقتطاع رسما ضريبيا عائدا للخزينة العامة في مقابل ما توفره الدولة من تنظيم و حماية لهذا النشاط.

أمـــا عـــن الجانـــب الإجرائـــي:

فإننا نرى أن المنظومة التشريعية يجب أن يطالها التحديث و إلا فإن تمسكها بالقواعد الإجرائية التقليدية لن يكون ذا فائدة ترجى، حيث أنها بوضعها الحالي أعجز عن أن تنطبق..... نصوصها على جرائم بهذه الطبيعة و الخصوصية بالدعوة قائمة و حبذا أن تكون الاستجابة لها على الفور أن يشمل التحديث قواعد بذات طبيعة جرائم التجارة الالكترونية و بذات خصوصية مجرميها حيث المجرم لا يترك أثرا كما أن أدلة الجريمة متخفية أو ليست من طابع مادي مثلما أن رجال الجهات القضائية يجب أن ينالوا حظهم من التدريب و التكوين الكفء في هذا المجال (مجال المعلوماتية) لما يتطلبه مرحل الاستدلال و التحقيق و إجراءات السابقة عن المحاكمة و التي تليها من إدراك و إتقان لتقنية الرقمية، كما أن هذا التكوين يجب أن يطال القضاة أيضا فلا تغني الخبرة في هذا المجال عن عمل القاضي، و لئلا يتقزم دور القاضي إلى ناقل لمعلومات الخبير.

إن القواعد الإجرائية الجنائية المعملة و المحكمة أو التي ينبغي أن تحكم أو تعمل تختلف عن تلك التي هي معملة في بيئة الجرائم التقليدية لما تتميز به الجرائم من النوع الأول من عدم اتصافها بالعنف التي تتصف به غيرها من الجرائم، كما أن الأسباب و العوامل التي تدفع إلى ارتكابها جرائم التجارة الالكترونية تختلف عنها في الجرائم التقليدية، حيث مجرد إثبات الذات و إظهار الكفاءة، القدرة على التحدي سبب كان لارتكاب هذه الجرائم، و هي ميزة انعكست على..... هذه البيئة فالبواعث التي تحركه حال ارتكابه لمثل هذه الجرائم تختلف عنها عند المجرم التقليدي و الأغرب هو ردة فعل المجني عليه تجاه أي سلوك جرمي يرتكب ضده و ما تولد لديه من خشية وخوف على السمعة.

و لعل أكبر الفوارق التي ميزت الجريمة في بيئة التجارة الالكترونية هي تخطيها للحدود الجغرافية، و اكتسابها بذلك طبعة عالمية دولية مما فرض على الدول حتمية التعاون فيما بينها.

وجب لأجل ذلك إيجاد رسائل مناسبة تتوافق فيها التشريعات بخصوص هذه الجرائم و بخاصة أن هذه الدول قد تعاونت فيما قبل و وحدت جهودها و قدمت تنازلات لم يكن من قبل تتصور أن ينزل إليها و لو تعلق بعضها بفواصل و حدود سيادية لأجل توحيد نظم و تشريعات تعلقت بالنشاط التجاري و هي في ذلك لها سابقة و تجربة فلا ضير أن تعيد و تحاول مرة أخرى تجربة التصدي لتلك الجرائم التي تهدد النشاط الذي ناضل لأجل تشييد صرح له و يسمى بالمنظمة العالمية للتجارة.

ضرورة مراعاة التطور المستمر الذي يطرأ على تكنولوجيا لمعاملات الرقمية و حول النصوص المنظمة لها أكثر مرونة و استيعاب لحركيتها المستمرة.

التوصيـــات و المقترحـــــات:

- تحديث النظم الإجرائية الحالية بما يتوافق و خصوصية الإجراءات الواجب اتخاذها للتصدي لجرائم التجارة الالكترونية على وجه الخصوص فيما يتعلق بنصوص الضابطة لإجراء التفتيش و ضبط نظم المعالجة الآلية و نظم الحاسب الآلي.

- إنشاء أقسام متخصصة بأكاديمية الشرطة لدراسة صعوبات التحقيق، و الاستعانة بالخبرة المحلية و الدولية لتدريب الطلاب على كيفية التعامل معها بطريقة فنية صحيحة لتلافي الإهمال أو إغفال الأدلة أو إتلافها و إفسادها[1] و تدعيم هذا التكوين بتكثيف الدراسات التدريبية بشكل دوري يلاءم تطورات التقنيات الإجرامية حتى يتمكن رجال أجهزة العدالة (رجال الضبطية، محامون، قضاة...) من التحقيق في القضايا بشكل فني موازي لذلك الذي سترتكب به الجرائم أو يزيد عنه.

- الدعوة إلى تحديث القانون الجنائي للنظم سواء ما تعلق بالنصوص التجريمية أو العقابية أي يطال هذا التحديث، الجوانب الموضوعية و الجوانب و الجوانب الإجرائية في إطار مسايرة التطورات التكنولوجية و تفاعل النشاط الإنساني مع تكنولوجيا الاتصال و المعلوماتية.

بحكم أن قواعد القانون الجنائي التقليدي غير كافية لمواجهة ما استحدث من جرائم على مستوى تقنية المعاملات التجارية الالكترونية، و هذا ما يعني وجود فراغات قانونية محتملة في عدد معين من مجالات التعامل بهذا النشاط، و ما يترتب عن ذلك عدم كفاية تلك النصوص أو انعدام وجود حماية أصلا لمصالح قانونية وجب كفالة حق الحماية لها، و إلا عد هذا الأمر قصورا تشريعيا و قد يكون السبيل إلى تدارك هذا العجز أو الفراغ بإحدى وسيلتين:

الأولى: إحداث تعديلات على النصوص القائمة بما يمكنها من استيعاب أو شمول الحماية التي تقررها للمراكز التقليدية لتمتد إلى أن تشمل بحمايتها مصالح مستحدثة بفعل التعامل بهذه التقنية في إطار تحديث المنظومة الجنائية.

الثانية: إفراد قوانين جديدة تتعلق..... بتنظيم هذه المعاملات و تنزيل أحكامها على غرار المشرع العربي و الدولي (تونس، الإمارات، الأردن، البحرين... قانون النموذجي للأمم المتحدة) كما يضمنها النصوص العقابية و القواعد الإجرائية.

- ضرورة انتهاج نهج ردعي في إطار العقوبات التي يقررها المشرع كجزاء لسلوكيات الإجرامية و ذلك بقدر الضرر الناتج عن هذه السلوكيات اللامادية و ما يخلفه من آثار سلبية مادية تهدد به مصالح و مراكز قانونية قائمة.

[1]- عفيفي كامل، ص 360

- دعوة المشرع الجزائري إلى استكمال ما بدأه من خطوات في إطار تحديث منظومته التشريعية، ذاك أن هذه البوادر مثنى عليها، لكنها غير كافية فالتقنية لا تنتظر إذ هي تتسارع و معها تتسارع الظاهرة الإجرامية، و الأفضل اتخاذ تدابير وقائية خير من إفراد التدابير العقابية البعدية، لتتمكن كل منظوماته من الاستفادة من التقدم التكنولوجي و تأمين مخاطره.

- تفعيل دور التعاون الدولي

- إيجاد تنسيق و تعاون دولي لتوحيد جزء من تشريعاتها فيما يتعلق بتعريف جرائم هذا النوع، و عدم اشتراط ازدواج التجريم على الأقل فيما يخص شبكة المجرمين.

- أن يستهدف هذا التفعيل تعزيز الإجراءات القانونية فيما تعلق بضبط الجناة، إقامة الدليل المعلوماتي و قبول حجيته، تبادل المعلومات مع وجوب المحافظة على سريتها، تبادل الخبرات في إطار الجانب الإجرائي.

- إن الوصول إلى كشف الحقيقة في هذه الجرائم أو الاستدلال عليها يكون صعبا و أحيانا مستحيلا دون تعاون وسطاء الخدمة بين المتعاملين التجاريين لذلك فإنه من الضروري وضع نص قانوني يلزم بمقتضاه وسطاء الخدمة (مورد الخدمات، مزود خدمات...) و العاملين على النظام المعلوماتي بالتعاون لكامل الجهات القضائية و سلطات التحقيق لضبط البيانات التي تدخل في نطاق الاستدلال بما لا يتعارض أو يصطدم بالحقوق المقرة دوليا و إقليميا و دستوريا أي الحق في الحياة الخاصة.

قائمة المراجع

I-المراجع باللغة العربية

1-الكتب المتخصصة :

01. إبراهيم العيسوي، التجارة الالكترونية، الطبعة الأولى, الملكية الأكاديمية, القاهرة 2003.

02. إبراهيم دسوقي أبو الليل، الجوانب القانونية للتعاملات الالكترونية، دون طبعة, لجنة التأليف و التعريف و النشر، مجلس النشر العلمي، جامعة الكويت، الكويت2003.

03. أحمد خليفة الملط، الجرائم المعلوماتية، دراسة مقارنة، دون طبعة، دون دار نشر2005.

04. أسامة أبو الحسن مجاهد، التعاقد عبر الانترنيت، دون طبعة, دار الكتب القانونية، القاهرة 2005.

05. أسامة أحمد المناعسة و جلال محمد الزعبي و صايل فاضل الهواوشة، جرائم الحاسب الآلي و الانترنيت – دراسة تحليلية مقارنة–، الطبعة الأولى، دار وائل، عمّان 2001.

06. أسامة أحمد بدر، حماية المستهلك في التعاقد الإلكتروني – دارسة مقارنة –، دون طبعة، دار الجامعة الجديدة للنشر، الاسكندرية 2005.

07. أشرف توفيق شمس الدين، الحماية الجنائية للمستند الالكتروني، – دراسة مقارنة – الطبعة الأولى، دار النهضة العربية، القاهرة 2006.

08. آمال قارة، الحماية الجزائية المعلوماتية في التشريع الجزائري ، الطبعة الثانية, دار هومه، الجزائر، 2006.

09. إيهاب فوزي السقا، جريمة التزوير في المحررات الالكترونية، دون طبعة، دار الجامعة الجديدة الإسكندرية 2008.

10. باسم الفقير، التزوير الالكتروني، الطبعة الأولى, دار اليراع للنشر والتوزيع، دمشق2007.

11. بلال أمين زين الدين، جرائم نظم المعالجة الآلية للبيانا ت في التشريع المقارن و الشريعة الإسلامية، دون طبعة، دار الفكر الجامعي، الإسكندرية 2008.

12. ثروت عبد الحميد، التوقيع الالكتروني ماهيته، مخاطره وكيفية مواجهتها مدى حجيته في الإثبات، دون طبعة، دار الجامعة الجديدة، الإسكندرية 2007.

13. جميل عبد الباقي الصغير، أدلة الإثبات الجنائي و التكنولوجيا الحديثة (أجهزة الرادار– الحاسبات الآلية – البصمة الوراثية) دراسة مقارنة، دون طبعة, دار النهضة العربية، القاهرة 2002.

14. جميل عبد الباقي الصغير، الجوانب الإجرائية للجرائم المتعلقة بالانترنيت، دون طبعة، دار النهضة العربية، 2002.

15. خالد مصطفى فهمي، النظام القانوني للتوقيع الالكتروني في ضوء التشريعات العربية والاتفاقيات الدولية، الطبعة الأولى، دار الجامعية الجديدة، الإسكندرية 2007.

16. خالد ممدوح إبراهيم، إبرام العقد الالكتروني دراسة مقارنة، دار الفكر الجامعي، الإسكندرية 2006.

17. خالد ممدوح إبراهيم، لوجيستات التجارة الالكترونية، طبعة أولى، دار الفكر الجامعي، الإسكندرية 2008،

18. شيماء عبد الغني محمد عطاالله، الحماية الجنائية للتعاملات الإلكترونية، بدون طبعة, دار الجامعة الجديدة، الإسكندرية 2007.

19. صالح المنزلاوي، القانون الواجب التطبيق على عقود التجارة الالكترونية، دار الجامعة الجديدة للنشر، الإسكندرية، 2006.

20. طارق إبراهيم الدسوقي عطية، الأمن المعلوماتي, النظام القانوني للحماية المعلوماتية، دار الجامعة الجديدة، الاسكندرية2009.

21. طارق عبد العالي حماد، التجارة الإلكترونية، الدار الجامعية، الاسكندرية 2003.

22. عبد الفتاح بيومي حجازي، التجارة الالكترونية في القانون العربي النموذجي لمكافحة جرائم الكمبيوتر، دون طبعة، دار الكتب القانونية– دار الشتات للنشر و البرمجيات, القاهرة 2007.

23. عبد الفتاح بيومي حجازي، التجارة الالكترونية وحمايتها القانونية، الطبعة الأولى، الجزء الثاني، دار الفكر الجامعي، الاسكندرية.

24. عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر و الانترنيت، دون طبعة، دار الكتب القانونية, القاهرة 2004 .

25. عبد الفتاح بيومي حجازي، حماية المستهلك عبر شبكة الإنترنيت، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية2006.

26. عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت، دون طبعة، دار الكتب القانونية– دار الشتات للنشر و البرمجيات, القاهرة 2007.

27. عبد الفتاح بيومي حجازي، مقدمة في التجارة الإلكترونية العربية، الجزء الثاني، دون طبعة, دار الفكر الجامعي، الاسكندريّ 2004.

28. عبد الوهاب ابراهيم أبو سليمان، البطاقات البنكية الإقراضية والسحب المباشر من الرصيد ، طبعة أولى، دار القلم ، دمشق1998.

29. عصام عبد الفتاح مطر، التجارة الالكترونية في التشريعات العربية و الأجنبية، دار الجامعة الجديدة، الإسكندرية 2009.

30. عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف و المصنفات الفنية ودور الشرطة و القانون، منشأة المعارف، الإسكندرية, دون سنة نشر.

31. علاء محمد نصيرات، حجية التوقيع الالكتروني في الإثبات (دراسة مقارنة)، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمّان 2005.

32. علي عبد القادر قهوجي، الحماية الجنائية لبرامج الكمبيوتر، دون طبعة, الدار الجامعية للطباعة و النشر، بيروت 1999.

33. علي كحلون، المسؤولية المعلوماتية، محاولة لضبط مميّزات مسؤولية المتدخلين في إطار التطبيقات المعلوماتية و خدماتها، دون طبعة، مركز النشر الجامعي، دون بلد نشر، 2005.

34. عماد حداد، التجارة الالكترونية، سلسلة كويك نوتس، دار الفاروق, اللجنة العلمية للتأليف والتحرير والنشر.

35. عمر حسن المؤمني، التوقيع الالكتروني وقانون التجارة الالكترونية، دراسة قانونية وتحليلية مقارنة، الطبعة الأولى, دار وائل للنشر والتوزيع، عمّان 2003.

36. فرج عبد العزيز عزت، اقتصاديات البنوك، دون طبعة، دون دار نشر، دون بلد نشر, 2000.

37. فيصل سعيد الغريب، التوقيع الالكتروني وحجيته في الإثبات، دون طبعة, منشورات المنظمة العربية للتنمية الإدارية، بحوث ودراسات، القاهرة 2005.

38. محمد إبراهيم أبو الهيجاء، عقود التجارة الالكترونية، الطبعة الأولى، دار الثقافة للنشر و التوزيع، عمان 2004.

39. محمد المرسي زهرة، الحماية المدنية للتجارة الالكترونية (العقد الالكتروني – الإثبات الالكتروني – المستهلك الالكتروني)، الطبعة الأولى، دار النهضة العربية, القاهرة 2008.

40. محمد حسن رفاعي العطار، البيع عبر شبكة الانترنيت دراسة مقارنة في ضوء قانون التوقيع الالكتروني رقم (15) لسنة 2004.

41. محمد حسين منصور، المسؤولية الالكترونية، دون طبعة, دار الجامعة الجديدة للنشر، الإسكندرية 2003.

42. محمد عبيد الكعبي, الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الانترنيت (دراسة مقارنة), دون طبعة, دار النهضة العربية, القاهرة 2005

43. محمود الكيلاني، الموسوعة التجارية و المصرفية, المجلد الثاني، التشريعات التجارية و الالكترونية (دراسة مقارنة)، الطبعة الأولى، دار الثقافة للنشر و التوزيع، عمّان2007.

44. مدحت عبد الحليم رمضان، الحماية الجنائية للتجارة الالكترونية، دون طبعة, دار النهضة العربية, القاهرة.

45. ممدوح محمد علي مبروك، مدى حجية التوقيع الالكتروني في الإثبات, دراسة مقارنة بالفقه الإسلامي, دون طبعة, دار النهضة العربية، القاهرة 2005.

46. موسى خليل متري ،القواعد القانونية الناظمة للصيرفة الإلكترونية، الجديد في أعمال المصارف من الوجهتين القانونية و الاقتصادية، الجزء الأول.

47. نبيلة هروال، الجوانب الإجرائية لجرائم الانترنت في مرحلة جمع الاستدلالات، الطبعة الاولى، دار الفكر الجامعي، الإسكندرية 2007 .

48. نجوى أبو هيبة، التوقيع الالكتروني تعريفه، مدى حجيته في الإثبات، دون طبعة, دار النهضة العربية، القاهرة 2003.

49. نضال سليم برهم، أحكام عقود التجارة الالكترونية، الطبعة الأولى، دار الثقافة للنشر و التوزيع، عمان 2009.

50. نعيم مغبغب، مخاطر المعلوماتية والإنترنت–المخاطر على الحياة الخاصة و حمايتها دراسة في القانون المقارن، دون طبعة، دون دار نشر1998.

51. نهلا عبد القادر المؤمني، الجرائم المعلوماتية، الطبعة الأولى، دار الثقافة النشر والتوزيع، عمّان 2008.

52. هدى حامد قشقوش، الحماية الجنائية للتجارة الالكرونية عبر شبكة الانترنت، دون طبعة, دار النهضة العربية، القاهرة 2000.

53. هدى حامد قشقوش، جرائم الحاسب الآلي في التشريع المقارن، دون طبعة, دار النهضة العربية، القاهرة 1992.

54. هشام فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية – دراسة مقارنة–، دون طبعة, مكتبة الآلات الحديثة، أسيوط 1994.

55. هلالي عبد اللاه أحمد، تفتيش نطم الحاسب الآلي و ضمانات المتهم المعلوماتي، دراسة مقارنة، الطبعة الأولى، دار النهضة العربية، القاهرة 1998.

56. هلالي عبد اللاه أحمد، حجية المخرجات الالكترونية في المواد الجنائية، دراسة مقارنة، الطبعة الأولى، دار النهضة العربية، القاهرة1997.

57. هلالي عبد اللاه أحمد , اتفاقية بودابست لمكافحة جرائم المعلوماتية،الطبعة الأولى، دار النهضة العربية، القاهرة2007.

الرسائل الجامعية :

رسائل الماجستير:

01. أمين اعزان، الحماية القانونية للمستهلك في مجال التجارة الإلكترونية عبر شبكة الإنترنيت ــ رسالة ماجستير،
معهد البحوث والدراسات العربية، جامعة الدول العربية، القاهرة 2003.

02. جميل محمد بني يونس, الحماية المدنية لبرامج الحاسب الآلي (دراسة قانونية مقارنة), رسالة ماجستير, جامعة عمان العربية, الاردن2003.

03. جميل محمد بني يونس, الحماية المدنية لبرامج الحاسب الآلي (دراسة قانونية مقارنة), رسالة ماجستير, جامعة عمان العربية, الاردن2003.

04. خثير مسعود، الحماية الجنائية لبرامج الحاسب الآلي، رسالة ماجستير، كلية الحقوق، جامعة تلمسان، الجزائر 2008.

05. عبد الله حسين عارف الشياب، التنظيم القانوني لبرامج الحاسب الآلي في التشريع الأردني(دراسة مقارنة), رسالة ماجستير, جامعة آل البيت, المفرق, الاردن2005.

06. محمد مسعود محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري و المقارن، رسالة ماجستير، كلية حقوق، الإسكندرية 2006.

07. محمد موسى محمد خلف, التعاقد بواسطة الإنترنيت(دراسة مقارنة تحليلية)، رسالة ماجستير في القانون، جامعة القدس, فلسطين2004.

08. يونس خالد عرب مصطفى، جرائم الحاسوب، رسالة ماجستير، الجامعة الأردنية، عمان1994.

أطروحات الدكتوراه:

01. أحمد حسام طه تمام ، الجرائم الناشئة عن استخدام الحاسب الآلي (الحماية الحماية الجنائية للحاسب الآلي) دراسة مقارنة، أطروحة دكتوراه كلية الحقوق،جامعة طنطا, مصر2000.

02. إيمان مأمون أحمد سليمان الجوانب القانونية لعقد التجارة الالكترونية، رسالة دكتوراه، كلية الحقوق، جامعة المنصورة، 2006.

03. خالد ممدوح إبراهيم ، إبرام العقد الإلكتروني، أطروحة دكتوراه، كلية الحقوق، جامعة الإسكندرية 2005.

04. علي حسن محمد الطوالبة, التفتيش الجنائي على نظم الحاسوب والإنترنيت(دراسة مقارنة), أطروحة دكتوراه, جامعة عمان العربية, الاردن2003.

05. عمر محمد أبوبكر بن يونس، الجرائم الناشئة عن إستخدام الانترنت، أطروحة دكتوراه، جامعة عين شمس، القاهرة2004.

06. عيسى غسان عبد الله الربضي، القواعد الخاصة بالتوقيع الالكتروني، أطروحة دكتوراه كلية حقوق، جامعة عين شمس, القاهرة2006.

07. غازي عبد الرحمان هيان الرشيد, الحماية القانونية من جرائم المعلوماتية (الحاسب و الانترنيت), أطروحة دكتوراه, الجامعة الإسلامية, لبنان 2004.

08. محمد أحمد محمد نور جستنية، مدى حجية التوقيع الالكتروني في عقود التجارة الالكترونية، أطروحة دكتوراه، كلية الحقوق، جامعة القاهرة، القاهرة 2005.

09. محمد سعيد أحمد إسماعيل، أساليب الحماية القانونية لمعاملات التجارة الالكترونية، أطروحة دكتوراه، كلية الحقوق، جامعة عين شمس، 2005.

أعمال المؤتمرات و الملتقيات:

01. أحمد شرف الدين، الجوانب القانونية للتجارة الالكترونية وآليات تسوية منازعاتها, مؤتمر الاعمال المصرفية الإلكترونية بين الشريعة و القانون, كلية الشريعة والقانون و غرفة تجارة وصناعة دبي, جامعة الإمارات العربية المتحدة, 9-11ربيع الأول 1424الموافق 10-12مايو2003, دبي2003.

02. أحمد شرف الدين، الجوانب القانونية للتجارة الالكترونية و آليات تسوية منازعاتها، أوراق ندوة عقود التجارة الالكترونية و منازعاتها، العقود و الاتفاقات في التجارة الالكترونية، من تنظيم المنظمة العربية للتنمية الإدارية، جامعة الدول العربية، القاهرة، 2007.

03. عزت محمد علي البحيري, القانون الواجب التطبيق على المعاملات الإلكترونية(نظرة عامة), مؤتمر الاعمال المصرفية الإلكترونية بين الشريعة و القانون, كلية الشريعة والقانون و غرفة تجارة وصناعة دبي, جامعة الإمارات العربية المتحدة, 9-11ربيع الأول 1424الموافق 10-12مايو2003, دبي2003.

04. سمير برهان، إبرام العقد في التجارة الالكترونية، أوراق ندوة عقود التجارة الالكترونية و منازعاتها، المنظمة العربية للتنمية الإدارية، القاهرة2007.

05. مدوخ ماجدة، الصيرفة الالكترونية، ماهيتها مخاطرها وتنظيمها القانوني، الملتقى الوطني حول المنظومة المصرفية في الألفية الثالثة (منافسة مخاطر و تقنيات) 6-7 جوان 2005، جامعة جيجل.

06. رحيم حسين, معراج هواري، الصيرفة الإلكترونية كمدخل لعصرنة المصارف الجزائرية أشغال ملتقى المنظومة المصرفية الجزائرية و التحولات الاقتصادية- واقع و تحديات، جامعةالشلف2004.

07. محمود أحمد إبراهيم الشرقاوي، مفهوم الاعمال المصرفية الالكترونية و أهم تطبيقاتها، مؤتمر الاعمال المصرفية الالكترونية بين الشريعة و القانون, كلية الشريعة والقانون و غرفة تجارة وصناعة دبي, جامعة الإمارات العربية المتحدة, 9-11ربيع الأول 1424الموافق 10-12مايو2003, دبي2003.

08. أحمد عبد الخالق، البنوك و التجارة الالكترونية، الجديد في أعمال المصارف من الوجهتين القانونية و الاقتصادية، أعمال المؤتمر العلمي السنوي لكلية الحقوق بجامعة بيروت العربية الجزء الثاني، منشورات الحلبي الحقوقية، بيروت.

09. عبد الله حسين علي محمود ، إجراءات جمع الأدلة في مجال جريمة سرقة المعلومات ، المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية ، أكاديمية شرطة دبي – مركز البحوث والدراسات 26- 2003/4/28 ، دبي– الأمارات العربية المتحدة ، مقال منشور بتاريخ: 2009/09/29، منتديات قوات الأمن المركزي، وزارة الداخلية، الجمهورية اليمنية على الموقع: http://www.yemencsf.org/vb/showthread.php?t=9666

10. محمد أبو العلا عقيدة، التحقيق وجمع الأدلة في مجال الجرائم الإلكترونية ، المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية ، أكاديمية شرطة دبي ، مركز البحوث والدراسات، 26-28 نيسان 2003 دبي – الإمارات العربية المتحدة، مقال منشور على موقع منتدى كلية الحقوق، جامعة المنصورة، مصر:
http://www.f-law.net/law/showthread.php/2208

11. شول بن شهرة، انعكاس ثورة المعلومات على الحقوق الفردية، الملتقى الوطني الأول حول الحقوق والحريات الفردية وآليات حمايتها في التشريع الجزائري في ظل العولمة، جامعة الاغواط، أفريل 2005.

12. أحمد عبد الكريم سلامة، الانترنيت و القانون الدولي الخاص فراق أم تلاق، مؤتمر القانون والكمبيوتر والإنترنت، كلية الشريعة والقانون،جامعة الإمارات العربية المتحدة، المجلد الثاني،الطبعة الثالثة 2004.

13. هلالي عبد الله أحمد، المؤتمر، حجية المخرجات الكمبيوتيرية في المواد الجنائية، مؤتمر القانون والكمبيوتر والإنترنت.

14. هشام فريد رستم، الجرائم المعلوماتية-أصول التحقيق الجنائي الفني، مؤتمر القانون والكمبيوتر والإنترنت، كلية الشريعة والقانون،جامعة الإمارات العربية المتحدة، المجلد الثاني،الطبعة الثالثة 2004.

15. نبيل محمد صبح، حماية المستهلك في التعاملات الالكترونية، حلقة نقاشية حول مشروع قانون التجارة الالكترونية الكويتي، جامعة الكويت 2005.

المجلات:

01. تطار محمد منصف، " النظام المصرفي الجزائري و الصيرفة الإلكترونية"، مجلة العلوم الإنسانية ، العدد الثاني ،جوان2002، جامعة محمد خيضر ،بسكرة.

02. جلال الشافعي، "التجارة الالكترونية و الضرائب"، مجلة البحوث التجارية, جلمعة الزقازيق، العدد 02، السنة 2002.

03. خالد سعد زغلول، "الحماية القانونية للتجارة الالكترونية"، حلقة نقاشية حول مشروع قانون التجارة الالكترونية الكويتي ،مجلة الحقوق، السنة 2005، جامعة الكويت.

04. فوزي أوصديق، "إشكالية المعلوماتية بين الخصوصية وإفشاء الأسرار المهنية(السر البنكي نموذجا)"،مجلة دراسات قانونية، مركز البصيرة للبحوث والدراسات و الخدمات التعلية، العدد الثاني، سبتمبر 2008، الجزائر.

05. محمود الرشيدي، "الجرائم الالكترونية و التأمين الالكتروني"، مجلة قضايا ، المركز الدولي للدراسات المستقبلية، العدد11، السنة الأولى، نوفمبر2005.

القوانيـــــن :

01. القانون المدني الجزائري

02. قانون العقوبات الجزائري

03. الجريدة الرسمية الجزائرية

المراجع الالكترونية:

01. عز الدين كامل أمين، الصيرفة الإلكترونية, مقال متوفر على الموقع الالكتروني:
http://www.bankofsudan.org/

02. علي حسن الطوالبة, التعاون القضائي الدولي في مجال مكافحة الجرائم الالكترونية, متوفر على الموقع الالكتروني:
http://www.arriyadh.com/Economic/LeftBar/Researches/-.doc_cvt.asp

03. علي حسن الطوالبه , مشروعية الدليل الالكتروني المستمد من التفتيش الجنائي ، منتدى كلية الحقوق جامعة المنصورة , مصر، متوفر على الموقع الالكتروني:
http://www.f-law.net/law/showthread.php/34082-

04. فؤاد جمال، جرائم الحاسبات و الانترنيت، الجرائم المعلوماتية، مقال متوفر على الموقع الالكتروني: www.tasheraat.com

05. مغاوري شلبي، البنك المحمول و النقود الالكترونية، متوفر على الموقع الالكتروني:
http://www.islam-online.net/iol-arabic/dowalia/namaa-35/morajaat.asp

06. يونس عرب، التجارة الالكترونية، متوفر على الموقع الالكتروني:
www.arablaw.org

07. يونس عرب، موسوعة القانون الالكتروني، مجموعة ابحاث متوفر على الموقع الالكتروني:
www .arablaw.org

المراجع باللغة الأجنبية:

OUVRAGES :

01- André Bertrand, Thierre Piette-coudol, internet et le droit, que sais-je?, collection encyclopédique, Paris.

02- Andre Prum, Le commerce électronique en droit luxembourgeois, larcier, Paris2000.

03- florence Mas, la conclusion des contra du commerce électronique, LGDI, Paris2005.

04- frédéric-jerome pasier, Emanuel Jez, la criminalité sur intérnéte, colléction que sais-je?, puf, Paris 2000.

05- Isabelle Falque – Pierrotion, Internet Enjeux juridiques, Rapports official, Paris1997.

06- Jean-claude Hallouin et Hervé Causse, Le contrat électronique Au cœur du commerce électronique, Le doit de la distribution Droit commun ou droit spécial ? Université de Poitiers Collection de la Faculté de droit et des sciences social, LGDJ, Paris 2005.

07- Marie -pierre, fenoll-trousseau ,Gerard Haas ,Internet et protection des donnés personnelles ,litec ,Paris 2000.

08- Michelle Jean Baptist, Créer et exploitée un commerce électronique, Editions litec, Paris 1998.

09- Nathalie Mallet-poujol, la création multimédia et le droit, Litec, Paris 2000.

10-Thidant Verbiest, Le nouveau droit du commerce électronique, droit et technologies, larcier, L.G.D.J Paris 2006.

11-Thierry Piette Coudol, la signature électronique, éditions litec, Paris 2004.

12-Xavier Linant de bellefends, Le Droit du Commerce Electronique, collection "que sais-je", Edition puf, Paris 2005.

13-La loi au quotidien, l'internet, les pricipaux textes de loi,les edition des journaux officiels, Paris 2002.

ARTICLES :

01-Agathe Lepage, "Libertés sur l'Internet et cybercriminalité : les apports au droit pénal de la loi pour la confiance dans l'économie numérique du 21 juin 2004", Revue Droit pénal n° 12, Décembre 2004.

02-Agathe Lepage, " Réflexions de droit pénal sur la loi du 6 août 2004 relative à la protection des personnes à l'égard des traitements de données à caractère personnel", Revue Droit pénal n° 3, Mars 2005.

03-Bertrande Warusfel, "Aspects juridiques de la dématérialisation des échanges dans le commerce électronique", Revue petites affiches, Droit de l'informatique, n° 27, 06 février 2004.

04-Bruno P. Langlois, "La protection des marques sur internet : le législateur fédéral américain s'attaque à la cyberpiraterie", Revue Gazette du Palais, n° 202, 20 juillet 2000.

05-Christophe Caron, "Le risque de confusion, élément constitutif de la contrefaçon," Communication Commerce électronique" n° 2, Février 2007.

06-Christophe Caron, "Vers un droit pénal communautaire de la contrefaçon", Revue Communication Commerce électronique n° 6, Juin 2007.

07-Christophe Jamin, "L'efficacité au service de la justice (*) " , Revue Gazette du Palais, Procédure civile, 21 avril 2007.

08-Cyril Rojinsky, "Commerce électronique et responsabilité des acteurs de l'Internet en Europe", Revue Gazette du Palais, 24 juin 2000.

09-Danièle Véret et Carole Fongue, "La signature électronique va-t-elle révolutionner le formalisme des marchés publics" ?, Revue Gazette du Palais, 23 janvier 2001.

10- Dominique Davoust," La lutte contre le blanchiment de capitaux : une action menée au plan international, européen et national" , Revue petites affiches , Droit pénal des affaires, 05 août 2002.

11- Éric A. Caprioli, "Mesures techniques de protection et d'information des droits d'auteur", Revue Communication Commerce électronique n° 11, Novembre 2006.

12- Éric A. Caprioli, "Transparence et sécurité des informations financières par voie électronique dans le règlement AMF après l'arrêté du 4 janvier 2007", Revue Communication Commerce électronique n° 6, Juin 2007.

13- Éric caprioli, "La directive européenne n° 1999/93/CE du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques", Revue Gazette du Palais, 31 octobre 2000.

14- Hubert Bitan , "Le site de commerce électronique : approche technique et juridique", Revue Gazette du Palais, 18 avril 2000.

15- Michel Aujean, "L'évolution de la fiscalité en Europe sous l'impulsion de la Commission: 50 ans du Traité de Rome", Revue Gazette du Palais, Communautés européennes, n° 191, 10 juillet 2007.

16- Nathalie Dreyfus, "De la responsabilité des intermédiaires techniques : contrefaçon ou responsabilité civile ?" Revue Communication Commerce électronique n° 1, Janvier 2007.

17- Nicolas Mathey ,"Le commerce électronique dans la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique", Revue Contrats Concurrence Consommation n° 10, Paris,Octobre 2004.

18- Nicolas Mathey, "Le commerce électronique dans la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique", Revue Contrats Concurrence Consommation n° 10, Octobre 2004.

19- Philippe Boure, "Internet et la lutte contre la cybercriminalité", Revue Gazette du Palais, 23 janvier 2003.

20- Sylvain Martin, Arnaud TESSALONIKOS, "La signature électronique , premières réflexions après la publication de la directive du 13 décembre 1999 et de la loi du 13 mars 2000", Revue Gazette du Palais, 20 juillet 2000.

21-Thierry Piette-Coudol ,"L'écrit électronique et la signature électronique depuis la LCEN", Communication Commerce électronique n° 9, Paris, Septembre 2004.

ACTES DES CONGRES ET SEMINNAIRES:

01-Anne Troye-walker, Le cadre juridique du commerce électronique en Europe, Les premiers journées internationales du droit de commerce électronique, actes du colloque de nice des 23,24et25 octobre 2000 organisé par le département sciencees juridique de L'EDHEC et l'école du droit de l'entreprise de la faculté de droit de l'univérsité de montpellier, actualités de droit de l'entreprise, litec, Paris.

02-Philippe Tourneau, la Notin de Contrats électronique, Les deuxiemes journées internationales du droit de commerce électronique, actes du colloque de nice des 6 et7 novembre 2003, organisé par le département sciencees juridique de L'EDHEC et l'école du droit de l'entreprise de la faculté de droit de l'univérsité de montpellier, actualités de droit de l'entreprise, litec, Paris 2005.

03-Rob Van Esch, electronic contracting: the European approach, Les deuxiemes journées internationales du droit de commerce électronique, actes du colloque de nice des 6 et 7 novembre 2003, organisé par le département sciencees juridique de L'EDHEC et l'école du droit de l'entreprise de la faculté de droit de l'univérsité de montpellier, actualités de droit de l'entreprise, litec, Paris 2005.

04-Théo Hassler ,Les Donnés personnelles et la protéction des personnes, Les premiers journées internationales du droit de commerce électronique, actes du colloque de nice des 23,24et25 octobre 2000 organisé par le département sciencees juridique de L'EDHEC et l'école du droit de l'entreprise de la faculté de droit de l'univérsité de montpellier, actualités de droit de l'entreprise, litec, Paris 2002.

05-Michel Jaccard , Forme preuve et signature électronique, Aspects juridiques du commerce électronique, séminaire de l'association genevoise de droit des affaires, schulthess zurich, Publications du centre d'études juridiques européennes, Genève 2001.

06-Xavier Oberson, problèmes fiscaux posés par le développement du commerce électronique, Aspects juridiques du commerce électronique, séminaire de l'association genevoise de droit des affaires, schulthess Zürich, Publications du centre d'etudes juridiques européennes, Genève 2001.

CODES :

01-Code de Procédures Pénale, Dalloz, Édition 2009.

02-Code Pénale français, Dalloz, Edition 2009.

فـهـرس المـوضـوعـات

مقدمـة	أ – و
الباب الأول: الحماية الجنائية الموضوعية للتجارة الالكترونية	11
الفصل الأول: الإطار التنظيمي للتجارة الإلكترونية	13
المبحث الأول : ماهية المعاملات التجارية الالكترونية	15
المطلب الأول: التطور التاريخي لمعاملات التجارة الالكترونية	16
الفرع الأول : الاتفاقيـــات الدولية	17
الفرع الثاني : الأعمـــــال الدوليـــــة	18
المطلب الثاني : تعريـــف التجـــارة الالكترونيـــة	20
الفرع الأول : تعريـــف التجـــارة الالكترونيـــة فـــي المنظمـــات الدوليـــة	20
الفرع الثاني : على مستوى الصعيد الإقليمي و صعيد الهيئات المتخصصة	23
المطلب الثالث : خصائـــص التجـــارة الالكترونيـــة	25
الفرع الاول: خصائص متعلقة بأطراف العلاقة	25
الفرع الثاني: خصائص متعلقة بالمعاملة ذاتها	26
المبحث الثاني : أحكـــام عقـــود التجـــارة الالكترونيـــة	27
المطلب الأول : المقصـــود بالعقـــد الالكترونـــي	28
الفرع الأول : تعريف العقد الالكتروني	28
الفرع الثاني : خصائـــص العقـــد الالكترونـــي	30
المطلب الثاني : الإيجـــاب الالكترونـــي	33
الفرع الأول : عموميـــة الإيجـــاب الالكترونـــي	35
الفرع الثاني : لغـــة الإيجـــاب	36
الفرع الثالث : النطـــاق المكانـــي للإيجـــاب	37
المطلب الثالث: القبـــول الالكترونـــي	37
الفرع الأول : طـــرق التعبيـــر عـــن القبـــول	38
الفرع الثاني : تأكيـــد القبـــول عـــن أطـــراف العقـــد	40
المبحث الثالث : تنفيـــــذ العقـــــد الالكترونـــــي	40
المطلب الأول : التزامـــات البائـــع أو مـــورد الخدمـــة	41
الفرع الأول: الالتزامـــات بالتسليـــم أو أداء الخدمـــة	41
الفرع الثاني : مطابقـــة محـــل الإتفاق للمواصفـــات	42
الفرع الثالث: الالتـــزام بالضمـــان	43
المطلب الثاني : التزامـــات المشتـــري	46
الفرع الأول : الالتـــزام باستـــلام البضاعـــة	46
الفرع الثاني : التـــزام المشتـــري بالوفـــاء	47

المبحث الرابع : الوفاء في معاملات التجارة الالكترونية	48
المطلب الأول: ماهية الصيرفة الإلكترونية	48
الفرع الأول: مفهوم الصيرفة الإلكترونية	49
الفرع الثاني : وسائل الدفع الالكترونية	50
المطلب الثاني : المخاطر الناتجة عن الصيرفة الإلكترونية	54
الفرع الأول: المخاطر العملية	55
الفرع الثاني: مخاطر قانونية	56
المطلب الثالث : القواعد القانونية للحد من مخاطر الصيرفة الإلكترونية	57
الفرع الأول : نموذج لجنة بازل	57
الفرع الثاني : نموذج الاتحاد الأوروبي	60
الفرع الثالث : نموذج هونغ كونغ	62
المبحث الخامس : صور الحماية المدنية للتجارة الالكترونية	63
المطلب الأول : حماية التوقيع الالكتروني	65
الفرع الأول : تعريف التوقيع الإلكتروني	65
الفرع الثاني : شروط التوقيع الإلكتروني	70
الفرع الثالث : صور التوقيع الالكتروني	71
المطلب الثاني: حماية المستهلك في عقود التجارة الالكترونية	75
الفرع الأول : مفهوم المستهلك الإلكتروني	75
الفرع الثاني : قواعد حماية المستهلك في التشريعات المقارنة	79
الفصل الثاني: الاعتداء على نظام عمل التجارة الإلكترونية	83
المبحث الأول: ماهية جرائم التجارة الالكترونية	84
المطلب الأول: التعريف بجرائم التجارة الالكترونية	85
المطلب الثاني: جرائم التجارة الالكترونية في التشريعات المقارنة	87
المبحث الثاني : الاعتداءات الواقعة على مواقع التجارة الإلكترونية	89
المطلب الأول: الدخول غير المشروع لمواقع التجارة الإلكترونية	90
الفرع الأول : مفهوم الدخول إلى النظام والبقاء غير المشروع فيه	92
الفرع الثاني : جريمة الدخول و البقاء غير المشروعين في صورتها البسيطة	94
الفرع الثالث : جريمة الدخول إلى النظام أو البقاء غير المشروع في صورتها المشددة	95
المطلب الثاني : الاعتداء العمدي على سير نظام المعالجة المتعلقة بالتجارة الالكترونية	96
الفرع الأول : الركن المادي للجريمة	98
الفرع الثاني :الركن المعنوي	99
المطلب الثالث : الاعتداء العمدي على المعطيات	100
الفرع الأول: فعل الإدخال	101

الفرع الثاني: فعل المحو	102
الفرع الثالث: فعل التعديل	102
المطلب الرابع : المساس العمدي بالمعطيات خارج نظام المعالجة	103
الفرع الأول: الركن المادي	103
الفرع الثاني: الركن المعنوي	103
المطلب الخامس: العقوبات المقررة في التشريع الجزائري والتشريعات المقارنة	104
الفرع الأول : العقوبات الأصلية	105
الفرع الثاني: العقوبات التكميلية	106
الفرع الثالث : عقوبات الشخص المعنوي	107
الفرع الرابع : الشروع في الجريمة	109
الفرع الخامس : الاتفاق الجنائي	109
المبحث الثالث :الحماية الجنائية للبيانات الشخصية و الاسمية	110
المطلب الأول: الجرائم الواقعة على البيانات الشخصية والاسمية	110
الفرع الأول: التكييف القانوني لهذه الجرائم	111
الفرع الثاني: علاقة هذه الجرائم بمعاملات التجارة الالكترونية	116
المطلب الثاني: الحماية المقررة للبيانات الشخصية والاسمية	117
الفرع الأول : تجريم فعل سوء استخدام آلية المعالجة	117
الفرع الثاني : تجريم الاعتداء على مضمون البيانات ذاتها	122
المبحث الرابع : المسؤولية الجنائية لمقدمي الخدمات الوسيطة الخاصة بالإنترنيت	129
المطلب الأول : نطاق مسؤولية وسطاء الخدمة	130
الفرع الأول : موقف التشريع الأوروبي من مسؤولية وسطاء الخدمة	131
الفرع الثاني : موقف المشرع الجزائري من مسؤولية الوسطاء	135
الفرع الثالث : موقف الفقه من مبدأ مسؤولية الوسطاء	136
المطلب الثاني: توزُّع مسؤولية مقدمي الخدمات الوسيطة	138
الفرع الأول: مسؤولية الوسطاء حسب الأدوار	138
الفرع الثاني: قضايا تطبيقية للقضاء الفرنسي وتقديره	146
الفصل الثالث: جرائم الاعتداء على مضمون نشاط التجارة الإلكترونية	148
المبحث الأول : جرائم الأموال في نطاق التجارة الالكترونية	149
المطلب الأول : مدى اعتبار البرامج المعلوماتية موضوع لجرائم الأموال	151
الفرع الأول : صعوبة الحكم جريان جرائم الأموال على التجارة الالكترونية	151
الفرع الثاني : ظهور فكرة المنقول المعلوماتي في جرائم الأموال	152
المطلب الثاني : جريمة السرقة في مجال التجارة الالكترونية	155
الفرع الأول : مدى اعتبار البرنامج مالا بصدد جريمة السرقة	155

الفرع الثاني : مدى توافر أركان جريمة السرقة في مجال التجارة الالكترونية	158
المطلب الثالث: جريمة النصب في معاملات التجارة الالكترونية	162
الفرع الأول: جريمة النصب المعلوماتي في التشريعات المقارنة	163
الفرع الثاني: أركان جريمة النصب في مجال التجارة الالكترونية	165
المطلب الخامس : جريمة خيانة الأمانة في معاملات التجارة الالكترونية	169
الفرع الأول: إمكانية وقوع جريمة خيانة الأمانة في نطاق التجارة الالكترونية	169
الفرع الثاني : السلوك الإجرامي المعلوماتي في جريمة خيانة الأمانة	171
المبحث الثاني : الجرائم الواقعة على التوقيع الالكتروني	173
المطلب الأول : الدخول بطريق الغش على قاعدة بيانات تتعلق بالتوقيع الالكتروني	174
الفرع الأول : مفهوم بيانات التوقيع الالكتروني	175
الفرع الثاني : الركـــن المـــادي للجريمة	175
الفرع الثالث: الركـــن المعنـــوي للجريمة	176
المطلب الثاني: جريمة صنع أو حيازة برنامج لإعداد توقيع الالكتروني	176
الفرع الأول : الركن المادي	176
الفرع الثاني : الركـــن المعنـــوي	178
المطلب الثالث : جريمة تزوير التوقيع الالكتروني	178
الفرع الأول : الركن المادي	180
الفرع الثاني : الركـــن المعنـــوي	181
المطلب الرابع : جريمة فض مفاتيح التشفير الالكتروني	181
الفرع الأول : الركن المادي	182
الفرع الثاني: الركن المعنوي	183
المبحث الثالث : جرائم تزويـــر المحررات الالكترونية التجارية	183
المطلب الأول: موقف بعض التشريعات من جريمة تزوير المحررات الالكترونية	185
الفرع الأول : التكييف القانوني لجريمة تزوير المحررات الالكترونية	186
الفرع الثاني : موقف المشرع الجزائري من تزوير المحررات الالكترونية	189
المطلب الثاني: أركـــان جريمة تزوير المحررات الالكترونية	190
الفرع الأول : الركـــن المـــادي	191
الفرع الثاني: الركـــن المعنـــوي	196
المطلب الثالث: صور تزوير المحررات الالكترونية و بيان مشكلاتها	197
الفرع الأول : قصـــور تشريعات طـــرق التزويـــر التقليديـــة	197
الفرع الثاني : الطـــرق المعتمـــدة فـــي تزويـــر المحـــررات الالكترونيـــة	198
المطلب الخامس : جريمـــة استعمـــال المحـــررات المـــزورة الكترونيـــا	199
الفرع الأول : الركـــن المـــادي	200

الفرع الثاني : الركن المعنوي	203
المبحث الرابع حماية المستهلك في عقود التجارة الإلكترونية	203
المطلب الأول : تنوع حماية المستهلك في المعاملات الالكترونية	204
الفرع الأول : صـــور الحماية الجنائية للمستهلك الإلكتروني	204
الفرع الثاني : المسؤولية الجنائية عن الإخلال بالحق في الإعلام	205
المطلب الثاني : نماذج عن الحماية الجنائية للمستهلك	207
الفرع الأول : الحماية الجنائية لبيانات المستهلك الشخصية	207
الفرع الثاني : الحماية الجنائية ضد الغش التجاري والصناعي	208
الفرع الثالث : جريمة الاحتيال في عقود التجارة الإلكترونية	209
المبحث الخامس: جريمـــة التهـــرب الضريبـــي في المبادلة التجارية الإلكترونية	210
المطلب الأول : مشـــكلات فـــرض الضريبـــة عـــلى معامـــلات التجـــارة الالكترونيـــة	210
الفرع الأول: خصوصية الضريبة في معاملات التجارة الالكترونية	211
الفرع الثاني: الصعوبات العملية لفرض الضريبة	214
المطلب الثاني: حلول فرض الضريبة على المبادلات التجارية الالكترونية	216
الفرع الأول : أسلـــوب الحيـــاد الضريبـــي الالكترونـــي	216
الفرع الثاني :خلـــق ضرائـــب الكترونيـــة جديـــدة	217
الفرع الثالث : أسلـــوب الغيـــر محـــل الثقـــة الضريبيـــة	218
الباب الثاني: الحماية الجنائية الإجرائية للتجارة الالكترونية	220
الفصل الأول: بعض الجوانب الإجرائية لجرائم للتجارة الإلكترونية	222
المبحث الأول: الجوانب الإجرائية السابقة للمحاكمة	224
المطلب الأول: الدعوى الجنائية في جرائم التجارة الالكترونية	225
الفرع الأول: سلطات أجهـــزة الضبـــط القضائي	227
الفرع الثاني: الاختصاص الإقليمي في أعمال الضبط القضائي	229
الفرع الثالث: مبدأ التخصص في عمل الضبـــطية القضائية	232
الفرع الرابع: الحصـــول عـــلى الإذن القضائـــي	236
المطلب الثاني: نظـــام الإرشـــاد الجنائـــي عبـــر الانترنيـــت	238
الفرع الأول: المرشد الجنائي الالكترونية	239
الفرع الثاني: ضوابط عمل المرشد المعلوماتي	240
المطلب الثالث: مشكلات متعلقة بسلطات الاستدلال	241
الفرع الأول: الامتناع عن الإبـــــلاغ	241
الفرع الثاني : صعوبات خبرة سلطات الاستدلال والتحقيق	248
المبحث الثاني: الطبيعة الخاصة لإجراءات الدعوى في مجال التعاملات الالكترونية	252
المطلب الأول: خصوصية إجراءات التحقيق في بيئة التجارة الالكترونية	252
الفرع الأول: جواز التحريات التي لا تتعلق بحرمة الحياة الشخصية	252

الفرع الثاني : حرمة الحياة الخاصة للبيانات المعالجة آليا	253
المطلب الثاني: الاستعانة بمزود الخدمات للكشف عن هوية المشترك و حركة اتصالاته	253
الفرع الأول: السر البنكي نموذجا	255
الفرع الثاني: تجريم اعتراض الاتصالات الالكترونية	257
المطلب الثالث: تعاون مزودي الخدمات مع رجال الضبط القضائي	259
الفرع الاول: التزام مزود الخدمات بالتعاون مع رجال الضبط القضائي	259
الفرع الثاني: مدى التزام مزودي الخدمات بسرّ المهنة	264
الفرع الثالث: مراقبة الاتصالات الالكترونية	264
الفصل الثاني: خصوصية التفتيش و الضبط في جرائم التجارة الالكترونية	271
المبحث الأول : التفتيش في بيئة التجارة الالكترونية	272
المطلب الأول: مدى صلاحية معاملات التجارة الالكترونية لأن تكون محلا لهذا الإجراء	273
الفرع الأول : إتجاهات التشريعات المقارنة من المسألة	274
الفرع الثاني: تفتيش النظم المعلوماتية	277
الفرع الثالث: نطاق التفتيش	280
المطلب الثاني : خصوصية التفتيش في البيئة الالكترونية	281
الفرع الأول : مدى جواز التفتيش لضبط المعلومات	282
الفرع الثاني : اختلاف تفتيش و ضبط المعلومات المخزنة عن الاتصالات المباشرة	284
الفر ع الثالث : دور مزودي الخدمات في إجراءات التفتيش	285
المطلب الثالث : بعض القواعد المنظمة للتفتيش و الاعتراض و التسجيل	286
الفرع الأول : تفتيش النظام بناء على إذن	287
الفرع الثاني: تفتيش النظام بدون إذن	296
الفرع الثالث: حالة تفتيش الشبكة	303
المبحث الثاني: الضبط في بيئة التجارة الالكترونية	305
المطلب الأول: قواعد الضبط في مجال التعاملات الالكترونية	306
الفرع الأول: الضبط بالنسبة لبرنامج الحاسب	307
الفرع الثاني: الضبط بالنسبة لبيانات الحاسب الآلي	309
المطلب الثاني: موقف الفقه المقارن من ضبط الأدلة الالكترونية	310
الفرع الأول: الاتجاهات الفقهية	310
الفرع الثاني: موقف المشرع الجزائري	312
المبحث الثالث: بعض إشكالات الجوانب الإجرائية أثناء مرحلة المحاكمة	313
المطلب الأول: قواعد الاختصاص المتعلقة بجرائم التجارة الالكترونية	313
الفرع الأول: القضاء الأمريكي	315
الفرع الثاني: القضاء الانجليزي	316

الفرع الثالث: اجتهادات المشرع الفرنسي	317
الفرع الرابع: موقف المشرع الجزائري	319
الفرع الخامس: المسألة عند تشريعـــات أخـــرى	320
المطلب الثاني : خصائـــص المستخرجات الالكترونـــية	320
الفرع الأول: الدليـــل الالكترونـــي دليل علمـــي	321
الفرع الثاني: الدليل الالكتروني من طبيعة تقنية	321
الفرع الثالث: تنـــوع الدليـــل الالكترونـــي وتطوره	322
الفرع الرابع: استرجـــاع الدليـــل الالكترونـــي	322
الفرع الخامس : شروط قبول الدليل الالكتروني	323
المطلب الرابع : المخرجـــات الالكترونية في نظم الإثبات المقارنة	324
الفرع الأول: حجية المخرجات الالكترونية في التشريعات اللاتينية	326
الفرع الثاني: حجية المخرجات الالكترونية في التشريعات الانجلوسكسونية	328
الفرع الثالث: حجية المخرجات الالكترونية أمام القاضي الجنائي	329
المطلب الخامس : إشكالات الدليل الالكتروني في الإثبات	331
الفرع الأول : شروط قوة الإثبات للمخرجات الالكترونية أمام القاضي الجنائي	333
الفصل الثالث: الحماية الإجرائية لتعاملات التجارة الالكترونية في ضوء الاتفاقيات الدولية	335
المبحث الأول : مبادرات التشريعات لتقنين الإجراءات الجنائية للعالم الرقمي	336
المطلب الاول : الحلول المقترحة في ضوء التشريعات المقارنة	337
الفرع الأول : إجتهادات المشـــــرع الأوروبي	338
الفرع الثاني : إجتهادات المشرع الأمريكي	341
الفرع الثالث:إجتهادات المشرع العربي و الوطني	342
المطلب الثاني: الحلول المقترحة في ضوء الجهود الدولية	345
الفـــرع الأول : جهـــود الامم المتحدة	346
الفـــرع الثاني : جهود منظمة التعاون الاقتصادي والتنمية	348
الفـــرع الثالث: الجمعية الدولية لقانون العقوبات	349
الفـــرع الرابع: الأحكام الإجرائية لإتفاقيـــة بودابســـت 2001	352
المبحث الثاني : دور التعاون الدولي في مواجهة جرائم التجارة الالكترونية	362
المطلب الأول: ضرورة تحقيق التعاون الدولي	364
الفرع الاول: أهمية التعاون الدولي لمكافحة الجرائم المعلوماتية	364
الفـــرع الثاني: مبـــررات التعـــاون الـــدولي	368
الفرع الثالث : صعوبات تحقيق التعاون دولي	368
المطلب الثاني : مجال التعـــاون الدولـــي	372
الفرع الأول: الأحكـــام العامـــة المتعلقـــة بالتعـــاون الدولـــي	374

الفرع الثاني : تسليـــم المجرميـــن	375
الفرع الثالث : المساعـــدة القضائيـــة	378
خاتمـــة	384
قائمة المراجع	392
فهرس الموضوعات	407
مـــلاحق	

الملخص:

لقد أدى حجم التعامل الإنساني مع ظاهرة المعلوماتية في فترة حديثة و وجيزة إلى استحداث مصطلحات التعامل الإيجابي مع التقنية الرقمية كما هو الشأن في التجارة الالكترونية. على النقيض من ذلك، أضحى هناك كذلك تفاعل إنساني سلبي، ظهر في نمط جديد من الجريمة له تبعات عكسية أكثر خطورة من الظاهرة الإجرامية التقليدية. فإذا كان من المعلوم أن الجريمة قرينة التطور العلمي، فإنه من البديهي أن يتوازى ظهور أنماط جديدة من الجريمة مع التطور التكنولوجي، تتعلق بسرية المعلومات، الاعتداء على الخصوصيات، حماية المستهلك، تداول البيانات الخاصة و غيرها من الجرائم التي تضر بالحقوق المقررة للأشخاص و المحمية قانونا أصلا.

ليس هناك فرق جوهري بين النظام التجاري التقليدي وما استحدث من تقنية التعاملات التجارية الحديثة عدا آلية التعامل بارتكاز التجارة الإلكترونية على شبكة الإنترنيت – التي هي نظام معلوماتي يتم بواسطته المبادلة التجارية. بناء على ذلك، فإن هذا النظام أصبح في حاجة عاجلة إلى كفالة حماية جنائية. بقدر ما حمى المشرِّع المراكز القانونية الناشئة عن التجارة التقليدية، بقدر ما هناك مصالح ينبغي أن تحمى و حقوقا ينبغي أن تسنّ لها النصوص الكافلة لها تلك الحماية في ميدان التجارة الالكترونية، وهو ما وجدنا فيه مسوغا لطرح الإشكالية التي شكلت إطار الدراسة و هي:

كيف يمكن كفالة حماية جنائية فعّالة لمبادلات التجارة الالكترونية؟

وهو ما استدعى البحث في الآليات التي أعدتها التشريعات الدولية والإقليمية والوطنية في إطار سياسة جنائية تتصدى للأفراد و الجماعات الذين احترفوا الإجرام المعلوماتي وتخطوا به كل الحدود المشفرة.

RESUME:

a façon et l'ampleur du phénomène récent de l'informatisation dans un temps relativement court ont engendré la terminologie reflétant la réaction positive avec les techniques de numérisation telle que le e-commerce (ou commerce électronique).

Le contraste avec cet aspect positif réside en une nouvelle forme de criminalité plus dangereuse encore que les crimes traditionnels. S'il est bien connu que la criminalité suit le progrès technologique, cela veut dire l'apparition des nouveaux crimes avec ce progrès technologique concernant la confidentialité des informations, la vie privée, les droits du consommateur et tout ce qui pourra être une atteinte aux droits légaux des personnes.

A vrai dire, il n y a presque pas de différences profondes entre le système commercial traditionnel et les nouvelles techniques commerciales mise à part l'automatisation des transactions du e-commerce via internet. Sur ce fait, la prise en charge d'une protection juridique de cette automatisation est devenue un besoin pressant. De même que le législateur a protégé les centres légaux engendrés par le commerce traditionnel, de même qu'il y a des intérêts à protéger et des droits à préserver à travers des textes explicites assurant une telle protection dans le domaine du e-commerce. C'est de cette réflexion que notre problématique encadrant cette recherche a pris naissance, à savoir :

Comment peut-on assurer une protection juridique efficace aux transactions du commerce électronique?

Une telle problématique a exigé la recherche dans les mécanismes pratiqués par les législations nationales, régionales et internationales dans le cadre d'une politique juridique qui fait face aux personnes et aux groupes qui se sont spécialisés dans la criminalité informatique dépassant toutes les sortes de protections techniques possibles.