جامعة جيلالي ليابس – سيدي بلعباس –
كلية الحقوق والعلوم السياسية

أطروحة دكتوراه في العلوم – تخصص علوم قانونية فرع علوم جنائية –

الحماية الجزائية للتجارة الإلكترونية

تحت إشراف
الأستاذ الدكتور: بودالي محمد

من إعداد المترشح
حطاب كمال

أعضاء لجنة المناقشة

أ.د. معوان مصطفى	أستاذ التعليم العالي	جامعة سيدي بلعباس	رئيسا
أ.د. بودالي محمد	أستاذ التعليم العالي	جامعة سيدي بلعباس	مشرفا ومقررا
د. سعداوي محمد الصغير	أستاذ محاضر (أ)	جامعة بشار	عضوا مناقشا
د. عرباوي نبيل صالح	أستاذ محاضر (أ)	جامعة بشار	عضوا مناقشا

السنة الجامعية: 2016/2015

بسم الله الرحمن الرحيم

"وأنــزل الله عليــك الكتــاب والحكمــة وعلمــك مــا لــم تكــن تعلــم وكــان فضــل الله عليك عظيما".

جزء من الآية 113 من سورة النساء.

إهداء

أهدي هذا العمل إلى كل من أكن له الحب والتقدير والاحترام وأخص بالذكر:

والدي الكريمين حفظهما الله ورعاهما وأمد في عمرهما.

جدتي الغالية شفاها الله من كل داء وحفظها من كل سوء.

مقلتيّ ونور عيني ابنتي الحبيبتين، ورفيقة دربي وشريكة حياتي زوجتي، ووالديها الكريمين وكل أفراد عائلتها.

إخوتي وأخواتي وكل أفراد عائلتي كل باسمه.

أساتذتي الكرام، خاصة الأستاذ الدكتور بودالي محمد على تفضل سيادته أولا بقبول الإشراف على هذا العمل رغم انشغالاته العديدة، وثانيا على حسن توجيهه ونصحه طوال سنوات البحث، وثالثا على دعمه وإرشاده وتشجيعه وحسن تعامله، فكان نعم الأستاذ ونعم الصديق.

كما أهدي هذا العمل إلى كل أساتذة وطلبة وعمال كلية الحقوق والعلوم السياسية، وأخص بالذكر صديقي الأستاذ طيفوري زواوي، وصديقي الأستاذ يعيش مجيد.

كما أهدي جهدي هذا إلى كل عالم أو متعلم أو محب للعلم.

شكر وتقدير

أحمد الله عز وجل وأشكره سبحانه وتعالى على أن وفقني لإتمام هذا العمل "وما توفيقي إلا بالله عليه توكلت وإليه أنيب".

أتقدم بالشكر الجزيل إلى الأستاذ الدكتور بودالي محمد الذي أشرف على هذا العمل، رغم مشاغله الكثيرة، فلم يضنّ علي بنصائحه وتوجيهاته القيمة، وآرائه السديدة.

كما أتقدم بجزيل الشكر إلى الأساتذة الأفاضل أعضاء لجنة المناقشة، وأخص بالذكر الأستاذ الدكتور معوان مصطفى على قبوله ترأس هذه اللجنة، رغم مهامه وانشغالاته العديدة.

كما أشكر الدكتور سعداوي محمد الصغير والدكتور عرباوي نبيل من جامعة بشار على قبولهما مناقشة هذا العمل رغم انشغالهما وبعد المسافة.

لكم مني أساتذتي الكرام كل الشكر والاحترام والتقدير.

قائمة المختصرات
Liste des abréviations

بالعربية

أ	أستاذ
ج	جزء
ج ر	الجريدة الرسمية
دج	دينار جزائري
د م ج	ديوان المطبوعات الجامعية
ص	صفحة
ط	طبعة
ع	عدد
ق ا ج	قانون الإجراءات الجزائية الجزائري
ق ا ج ف	قانون الإجراءات الجزائية الفرنسي
ق ع	قانون العقوبات الجزائري
ق ع ف	قانون العقوبات الفرنسي
ق ع م	قانون العقوبات المصري
م	مادة
م3/5	الفقرة الثالثة من المادة الخامسة
م3/5-1	البند الأول من الفقرة الثالثة من المادة الخامسة
و م أ	الولايات المتحدة الأمريكية

بالفرنسية

Art.	Article
Cour de cassation chambre criminelle	Cass. Crim
Chambre	Ch.
Commission nationale de l'informatique et des libertés	CNIL
Fournisseur d'accès Internet	FAI
Haute autorité pour la diffusion des œuvres et protection internet	HADOPI
Ibidem (au même endroit)	Ibid.
Loi pour la confiance dans l'économie numérique	LCEN
Numéro	N
Opère citao (ouvrage cité)	Op cit
Page	p
Système de Traitement Automatisé de donnés	STAD
Tribunal	T.
Tribunal correctionnel	T.Corr.
Tribunal de grande instance	TGI

مقدمة.

عالم اليوم معقد جدا، ومتداخل مع بعضه بعضا، بلغ فيه التقدم العلمي والتقني مبلغا لم يبلغه من قبل، أزالت فيه تكنولوجيا المعلومات والاتصالات الحدود بين الدول، بحيث صار العالم كله بمثابة قرية صغيرة يعرف أقصاها أدناها، وتبوأت فيه المعرفة مكانة الصدارة، بحيث لم يعد الصراع في العالم مقتصرا فقط على من يملك ومن لا يملك، بقدر ما صار محتدما بين من يعرف ومن لا يعرف، وسادت مفاهيم العولمة في مجالات شتى، لعل أبرزها المجالات الاقتصادية والمالية، ووجدت بيئة جديدة أتاحت للمتعاملين وسائل متطورة للإعلان عن السلع والخدمات تمهيدا للتعاقد عليها، وتنفيذها أحيانا عبر النقل الآلي للبيانات المجسدة للأداء محل الالتزام، دونما ضرورة للتواجد الشخصي في موقع التعاقد أو التنفيذ، نظرا لما تتمتع به هذه التقنيات من سرعة تؤدي إلى توفير في الوقت والتكاليف وفتح آفاق وأسواق جديدة بسهولة ويسر، وبدأ الحديث عن التسوق الإلكتروني والمعارض الافتراضية، الأمر الذي يسمح بالقول بأن النظام المعلوماتي أثر في تغيير محل التجارة، وكذا الوسائل التي تتم بها هذه التجارة، مما مكن من إبرام الصفقات عن بعد وخاصة عبر شبكة الانترنت، وهو ما يطلق عليه على سبيل الشيوع "التجارة الإلكترونية" والتي غدت بحق حقيقة واقعية تكرس وجودها في الميدان يوما بعد يوم،[1] وأصبحت تعد أهم ملامح النظام الاقتصادي الجديد، وفرضت نفسها في الميدان خلال السنوات الأخيرة، وهي في نمو مستمر حيث يؤكد الخبراء أنها تتعاظم مع مرور الأيام.[2]

ولا تقتصر التجارة الإلكترونية على عمليات بيع وشراء السلع والخدمات عبر الانترنت، إذ توسعت لتشمل عمليات بيع وشراء المعلومات نفسها، وهي تقدم الكثير من المزايا، دعما للمبيعات وخدمة للعملاء، وما على العميل سوى اقتناء جهاز حاسب آلي، وبرنامج متصفح الانترنت، والاشتراك بالانترنت للتمتع بمزايا التجارة الإلكترونية.[3]

حسب دراسة قامت بها فدرالية التجارة الإلكترونية والبيع عن بعد، بلغ سنة 2011 حجم التجارة الإلكترونية في فرنسا 36.2 مليار يورو، بنسبة نمو قدرت ب: 22% عن عام 2010،

[1] محمد عبيد الكعبي، الحماية الجنائية للتجارة الإلكترونية، أطروحة دكتوراه في الحقوق، جامعة القاهرة، 2009، ص10.

[2] د. نزيه عبد المقصود محمد مبروك، المعاملة الضريبية لصفقات التجارة الإلكترونية، دار الفكر الجامعي، الإسكندرية، مصر 2010، ص3.

[3] د. مصطفى معوان، التجارة الإلكترونية ومكافحة الجريمة المعلوماتية، دار الكتاب الحديث، القاهرة 2009، ص23.

وارتفع عدد المستهلكين الإلكترونيين بـ: 11% بالمقارنة مع سنة 2010، ليبلغ سنة 2011 ثلاثين مليون فرنسي، كما تزايدت أعداد مواقع البيع عبر الانترنت بنسبة 27% لتصل سنة 2011 إلى 100400 موقع تجاري بفرنسا، وتم تسجيل 420 مليون صفقة تجارية سنة 2011 مقابل 340 مليون صفقة سنة 2010، ومن أشهر المواقع: تلك المتعلقة ببيع المواد على اختلافها ومواقع السياحة الإلكترونية؛ كما سجلت مبيعات الهاتف النقال عبر الانترنت سنة 2011 نسبة 3% من البيوع الإلكترونية، في ارتفاع ملحوظ،[1] وقد شهدت الهواتف النقالة الذكية نقلة نوعية، لا من حيث الطلب عليها فحسب، حيث تم حسب بعض المصادر بيع 671 مليون هاتف ذكي في العالم عام 2012، بزيادة 42% عن 2011،[2] بل كذلك من أجل استعمالها للإبحار عبر شبكة الانترنت، حيث تشير دراسة أجريت بفرنسا في مايو 2012 أن 14% من المتعاملين عبر شبكة الانترنت اشتروا حاجة لهم، أو تمتعوا بخدمة سفر، عن طريق هواتفهم النقالة الذكية، ويتوقع أن يتعاظم دور الهاتف النقال الذكي مستقبلا، ومن بين فوائده المرجوة بالنسبة للتجارة الإلكترونية أن يلعب دور بطاقة الوفاء عبر الانترنت.[3]

وتفيد الدراسات بأن البيوع عبر شبكة الانترنت في تزايد مستمر، ومن بين المواقع الأكثر زيارة على الانترنت في فرنسا موقع: Amazon، وموقع: eBay وموقع:cDiscount وموقع: Fnac ...[4]

في أوربا وحسب دراسة أجريت سنة 2012، بينت أن مجموع البيوع على شبكة الانترنت عرفت تزايدا ملحوظا في السنوات الأخيرة، ففي ألمانيا مثلا بلغت قيمة المبيعات على الانترنت 29.4 مليار يورو سنة 2008، لتقفز سنة 2012 إلى 50.92 مليار يورو.[5]

بعيدا عن القارة الأوربية، سجلت التجارة الإلكترونية نموا كبيرا في حجمها ففي الولايات المتحدة الأمريكية تجاوزت قيمة الصفقات التجارية الإلكترونية 100 مليار دولار عام 2006، بنسبة نمو قدرت بحوالي 24% عن عام 2005، وفي تقرير لمنظمة التجارة العالمية، أظهر أن حجم التجارة

[1] Romain.V.Gola, droit du commerce électronique, Gualino lextensoédition,Paris 2013,p14.

[2] د. حفيظ الزايدي، الآليات القانونية والإجرائية للحد من آثار الجريمة الإلكترونية على الائتمان المالي، سلسلة ندوات محكمة الاستئناف بالرباط، تأثير الجريمة الإلكترونية على الائتمان المالي، العدد السابع، مطبعة الأمنية، الرباط 2014، ص168.

[3] Romain.V.Gola,Op cit, p26.

[4] I bid, p15.

[5] I bid, p16.

الإلكترونية قارب 300 مليار دولار عام 2008، بنسبة نمو فاقت 15% عن العام الفارط،[1] وتشير الدراسات المتخصصة الصادرة من مجلس الوحدة الاقتصادية التابع لجامعة الدول العربية أن معدل نمو التجارة الإلكترونية العربية يقدر بحوالي 15% سنويا متأخرا عن معدل النمو العالمي البالغ 30% سنويا، وهو أمر يتطلب من الدول العربية أن تسعى جاهدة نحو خلق بيئة ملائمة للتجارة الإلكترونية في جميع المجالات، وخاصة المجال القانوني لتحقيق قفزة نوعية في مجال التجارة الإلكترونية، وتضييق الهوة بينها وبين بقية دول العالم.[2]

إن هذا التزايد الكبير في حجم التجارة الإلكترونية، يرجع بالأساس إلى شبكة الانترنت التي أحدثت ثورة في حياة الملايين عبر العالم، إذ أتاحت لهم إمكانيات هائلة في مجالات شتى كالتسويق والدعاية والإعلان والاتصالات والتبادل التجاري والثقافي، كما سمحت لأي مؤسسة أو شركة تجارية مهما كان حجمها أن تتحول إلى منشأة عالمية – ولو من حيث المبدأ – بمجرد أن تضع لنفسها موقعا إلكترونيا على شبكة الانترنت، بحيث يمكن للعالم بأسره التعرف عليها؛ وفي خلال فترة زمنية وجيزة انتشرت الانترنت بين الجماهير على اختلاف أعمارهم وأذواقهم انتشارا غير مسبوق، وساعد على هذا انخفاض أثمان المنتجات الخاصة بتكنولوجيا المعلومات، وسهولة استخدام الشبكة، خاصة بعد أن صممت شركة "مايكروسوفت" نظام التشغيل "ويندوز" وطورته باستمرار.[3]

إن شبكة الانترنت والتي تعني لغويا الترابط الذي يتم بين الشبكات، إذ تتكون من عدد كبير من شبكات الحاسب الآلي المترابطة فيما بينها والمتناثرة في أنحاء العالم كله، عبارة عن وسيلة تواصلية بين الشبكات المعلوماتية، دون أن تعير للحدود الدولية اهتماما، ورغم أنها من جذور عسكرية وجامعية، وتمت دون تصميم استراتيجي مسبق، إلا أنها باتت تلعب دورا رئيسا في عالم التطور السريع في الاتصالات والمواصلات؛ ولقد تم تمويل كلفة بنيتها التحتية بصورة تدريجية من طرف جهات وهيئات مختلفة تمتلك كل منها شبكتها الخاصة، ثم جرى توصيل هذه الشبكات لاحقا بشبكة الانترنت. [4]

---

[1] نزيه عبد المقصود، المرجع السابق، ص5.

[2] أمين أعزان، الحماية الجنائية للتجارة الإلكترونية، رسالة لنيل درجة دكتوراه في الحقوق، جامعة عين شمس، مصر (دون ذكر سنة المناقشة)، ص3.

[3] الكعبي، المرجع السابق، ص11. يراجع أيضا:

منير محمد الجنبيهي، ممدوح محمد الجنبيهي، الشركات الإلكترونية، دار الفكر الجامعي، الإسكندرية، مصر 2008، ص08.

[4] د. حسين بن سعيد الغافري، السياسة الجنائية في مواجهة جرائم الانترنت، دار النهضة العربية، القاهرة 2009، ص15.

في عام 1984 ولدت شبكة الانترنت رسميا بفضل اجتماع أربع شبكات اتصال هي: CSN, Bitnet, Usenet, Arpanet انضمت لها لاحقا شبكة NSFnet وأضحى بروتوكول TCP/IP ركيزة العمل في هذه الشبكة ولغة الاتصال الرقمي فيها، ومع نهاية عقد الثمانينيات قررت الولايات المتحدة الأمريكية، والتي كانت تحتضن الشبكة من خلال المؤسسة الوطنية للعلوم NSF، وقف توظيف واستثمار مواردها المالية في تطوير شبكة الانترنت فاسحة المجال أمام وسائل التمويل الأخرى لتستكمل بناء هذه الشبكة.[1]

إن الحقيقة الماثلة أمامنا، والتي لا ينكرها عاقل، أن شبكة الانترنت، لما تتميز به من خصائص، لها دور كبير في جميع مناحي الحياة المعاصرة، الثقافية، الاقتصادية بل وحتى السياسية، وأسهمت إسهامات بالغة في التقريب بين الشعوب، وكان لها مزايا كبيرة خاصة في مجال تطوير التجارة الإلكترونية، لكن في المقابل يستغلها البعض من أجل غايات غير نبيلة، ويسعون من خلالها إلى تحقيق مآربهم الدنيئة من خلال استغلال هذه الشبكة لتحقيق الأرباح غير المشروعة عن طريق الغش والاحتيال، بل والتجسس والإرهاب الإلكتروني...وليست التجارة الإلكترونية بمنأى عن هذه الجرائم الجديدة التي اصطلح عليها الجرائم الإلكترونية، أو الجرائم المعلوماتية- التي تتميز بسمات خاصة منها أنها عالمية، وأن مخاطرها أمنية مادية وفكرية، وأنها سهلة الارتكاب، وأن إخفاء معالم الجريمة أمر يسير، وأنه توجد صعوبة بالغة لتتبع مرتكبيها، وتحديد حجم الجريمة وحجم الضرر -[2] إذ من الوارد جدا أن يتعرض مستعملو الانترنت للنصب أو السرقة أو الابتزاز... بل أن الإحصاءات الرسمية تشير إلى التزايد الكبير للجرائم الواقعة على التجارة الإلكترونية خاصة على شبكة الانترنت، حيث يؤكد تقرير "نورتن" لسنة 2011 بأن عائدات الجرائم الالكترونية بلغت حوالي 388 مليار دولار أمريكي، ووصلت في فرنسا لوحدها إلى ما يناهز 2.5 مليار يورو، وتضرر من الجرائم الإلكترونية في هذه السنة (2011) حوالي عشرة ملايين فرنسي،[3] مما دعا المجتمع الدولي بأسره أن يفكر في توفير أنواع كثيرة من الحماية للتعاملات الإلكترونية، بدءا بالحماية الفنية، وانتهاء بالحماية القانونية، المدنية منها والجزائية، غير أن هناك مشكلات وتحديات اعترضت في البداية هذا المسعى،

[1] الغافري، المرجع السابق، ص18.

[2] ليلى الزوين، عرض حول الجرائم الإلكترونية المالية، سلسلة ندوات محكمة الاستئناف بالرباط، تأثير الجريمة الإلكترونية على الائتمان المالي، العدد السابع، مطبعة الأمنية، الرباط 2014، ص188.

[3] د. حفيظ الزايدي، المرجع السابق، ص168.

من أهمها عدم وجود جهات تحكم الانترنت، حيث أن هذه الأخيرة ليست مملوكة لشخص أو هيئة بعينها، بل للجميع، مما دعا البعض إلى القول أن الانترنت منطقة حرة،[1] لا تخضع للقانون، خاصة وأنها أول مؤسسة عالمية لا تملكها أية حكومة أو جهة معينة، ولا يوجد من يسيطر على نشاط الانترنت، وإن كان هنالك بعض الحكومات كالصين تحاول تقليل الاتصال بها،[2] غير أن القول بأن الانترنت لا تخضع لقانون فيه الكثير من الشطط، وتجاوزه الزمن مما جعل الدول بصفة فردية أو جماعية تسعى بالتدريج لوضع تنظيم قانوني للانترنت، والتغلب على المشاكل التي يمكن أن تثار بهذا الشأن، وظهر مشكل آخر هو تعدد القوانين – سواء على مستوى الدولة الواحدة، أو على المستوى العالمي– التي يجوز أن تخضع لها الانترنت، مما يستدعي التعاون الدولي في هذا المجال.

إن التجارة الإلكترونية موضوع من موضوعي ما يعرف بالاقتصاد الرقمي الذي يقوم أيضا على تقنية أو صناعة المعلومات، التي لها الفضل في إيجاد التجارة الإلكترونية، التي تمتد عموما إلى ثلاثة أنواع من الأنشطة، الأول خدمات ربط أو دخول الانترنت وما تتضمنه من خدمات ذات محتوى تقني، ومثالها الخدمات المقدمة من مزودي خدمات الانترنت، الثاني التسليم أو التزويد التقني للخدمات، أما الثالث فهو استخدام الانترنت كوسيلة لتوزيع الخدمات والبضائع المسلمة تسليما ماديا عاديا.[3]

وقد حققت التجارة الإلكترونية أنشطة واسعة على المستويات الدولية والإقليمية والوطنية، لذا بذلت مجهودات كبيرة لتنظيمها من الناحية القانونية، فعلى الصعيد الدولي كانت أكثر الجهود، تلك التي بذلتها لجنة قانون التجارة الدولية في الأمم المتحدة الأونسيترال (UNICITRAL)، اعتبارا من منتصف الثمانينيات في مجال البحث في مسائل التبادل الإلكتروني للرسائل، ليتوج الجهد عام 1995 بإقرار القانون النموذجي للتجارة الإلكترونية والمعروف بقانون الأونسيترال لسنة 1996، الذي يمثل الإطار التشريعي الأساس للتشريعات الوطنية في مجال التجارة الإلكترونية، وما يتفرع عنها من تشريعات، كتلك الخاصة بالتوقيعات الإلكترونية، أو البطاقات

[1] د. يوسف حسن يوسف، التجارة الالكترونية وأبعادها القانونية الدولية، المركز القومي للإصدارات القانونية، القاهرة 2011، ص180.

[2] د. خالد ممدوح إبراهيم، حجية البريد الإلكتروني في الإثبات، دراسة مقارنة، دار الفكر الجامعي، الإسكندرية، مصر 2010، ص25.

[3] د. يوسف حسن يوسف، المرجع السابق، ص161.

الائتمانية، أو شهادات التوثيق الإلكتروني وغيرها،[1] ومن ذلك تشريع الأونسيترال بشأن التوقيع الإلكتروني الصادر سنة 2001.

وبعد صدور قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية سنة 1996، سارعت العديد من الدول إلى إصدار قوانين تتعلق بالتجارة الإلكترونية مسترشدة في ذلك بهذا القانون، وتعتبر دولة سنغافورة أول دولة في العالم أصدرت قانونا للتجارة الإلكترونية على نهج قانون الأونسيترال النموذجي، كان ذلك سنة 1998، وتلتها بعد ذلك عدة دول منها الولايات المتحدة الأمريكية وإيطاليا سنة 1999، لتليها فرنسا، الصين وتونس عام 2000، ثم إمارة دبي، والبحرين عام 2002.[2]

لقد أدرك العالم ضرورة التعاون الدولي في مجال التجارة الإلكترونية، لذلك عمدت العديد من الدول إلى إبرام المعاهدات، وعقد المؤتمرات الدولية، ومحاولة التنسيق بين القوانين المختلفة للدول بغية مجابهة الجرائم المعلوماتية، ونسجل في هذا الصدد إبرام معاهدة بودابست لمكافحة جرائم الانترنت في أواخر سنة 2001، التي تهدف إلى توحيد الجهود الدولية لمكافحة جرائم الانترنت، خاصة وأنها أبرمت في فترة شهدت فيها الجرائم المعلوماتية طفرة واضحة، تمثلت في قيام مجرمين محترفين على درجة كبيرة من الخبرة والتخصص في المجال المعلوماتي بالاحتيال والاختلاس، وتهديد الحياة الخاصة، وهي قضايا خطيرة تعرض حياة وممتلكات الكثيرين للخطر؛[3] ووقع على الاتفاقية مسؤولون في الدول الأوربية بالإضافة إلى بعض الدول من خارج القارة العجوز مثل الولايات المتحدة الأمريكية، اليابان، كندا، وجنوب إفريقيا؛ ولقد بذلت مجهودات مضنية في سبيل إبرام هذه الاتفاقية، والتوقيع عليها من قبل كل الأطراف دون أن يعترض عليها أي طرف، ولتحظى بالقبول الدولي وتتوسع دائرة الدول التي توافق على الانضمام إلى المعاهدة مستقبلا.

---

[1] د. يوسف حسن يوسف، المرجع السابق ص164.

[2] عبد الوهاب مخلوفي، التجارة الإلكترونية عبر الانترنت، أطروحة دكتوراه في العلوم، تخصص حقوق، فرع قانون أعمال، جامعة الحاج لخضر، باتنة 2012/2011، ص18.

[3] منير محمد الجنبيهي، وممدوح محمد الجنبيهي، جرائم الانترنت والحاسب الآلي ووسائل مكافحتها، دار الفكر الجامعي، الإسكندرية 2006، ص180.

وقد تضمنت هذه الاتفاقية العديد من المواضيع المتعلقة بالجرائم الإلكترونية، منها الإرهاب الإلكتروني، وعمليات تزوير البطاقات الائتمانية، ودعارة الأطفال، وهي الجرائم الأكثر شيوعا على المستوى العالمي بصفة عامة، وفي أمريكا وأوربا بصفة خاصة،[1] حيث لم تفلح من قبل أية جهود فردية تم بذلها من جانب أي من الدول الموقعة على الاتفاقية أو دول أخرى لم توقع بعد، مما يجعل التعاون الدولي لمكافحة هذه الجرائم حتمية لا مفر منها.

وتحدد الاتفاقية أفضل الأساليب التي ينبغي اتباعها في التحقيق في الجرائم المعلوماتية التي تعهدت الدول الموقعة بالتعاون على محاربتها، رغم أن الكثير من المنظمات الحقوقية كانت تخشى من أن تحد الاتفاقية من حرية الأفراد خاصة وأنها أبرمت عقب الهجمات الإرهابية على الولايات المتحدة الأمريكية في سبتمبر 2001، وهو ما يتعارض مع الإعلان العالمي لحقوق الإنسان حسب بعض هذه المنظمات الحقوقية، كما أن مزودي خدمات الانترنت أبدوا قلقهم من شدة الرقابة التي ستفرض عليهم، غير أن المدافعين عن المعاهدة رأوا بأن لا غرض لها سوى احترام حقوق الإنسان، والحد من تعرض مستخدمي الانترنت للكم الهائل من الجرائم المرتكبة عبر الشبكة، وهي لا تتعارض مع الإعلان العالمي لحقوق الإنسان بل تدعمه.[2]

على الصعيد الأوربي تم إعداد المعاهدة الأوربية لمكافحة جرائم الانترنت، وسط انتقادات من دعاة المدافعين عن حقوق الإنسان، والهدف منها إلزام الدول الأطراف المصادقة عليها بسن الحد الأدنى من القوانين الضرورية للتعامل مع جرائم التقنية العالية بما في ذلك الدخول غير المشروع إلى مواقع الانترنت والتلاعب بالبيانات، وجرائم الاحتيال والتزوير المعلوماتي، وصور القاصرين الإباحية، وانتهاكات حقوق النسخ الإلكتروني، وتتضمن المعاهدة بنودا تكفل للحكومات حق المراقبة، وتلزم الدول بمساعدة بعضها بعضا في جمع الأدلة وفرض القانون.[3]

تعتبر الكيانات الاقتصادية من أهم الأهداف المحتملة للعمليات الإجرامية عبر الانترنت، وغالبا ما يكون الدافع من وراء ذلك، هو البحث عن أموال تلك الشركات، أو ما تخفيه من معلومات قيمة تحاول الشركات المنافسة الحصول عليها، أو لابتزاز هذه الشركات والحصول منها على

[1] طارق فوزي الفقي، الجوانب الإجرائية في الجرائم المعلوماتية، رسالة دكتوراه في الحقوق، جامعة المنوفية، مصر 2011، ص253.

[2] منير محمد الجنبيهي، وممدوح محمد الجنبيهي، المرجع السابق، ص185.

[3] منير محمد الجنبيهي، وممدوح محمد الجنبيهي، المرجع السابق، ص186.

مبالغ ضخمة، نظير عدم نشر أسرارها، مما دفع هذه الكيانات الاقتصادية لأن تتحد فيما بينها ضد هذه الأخطار المحدقة بها، وتجلت صورة هذا التعاون من خلال تبادل الخبرات بهدف توفير حماية فنية فعالة ضد مجرمي الانترنت.[1]

تعتبر الاعتداءات الواقعة على الملكية الفكرية من خلال الانترنت من أكثر الأمور التي تستدعي التعاون العاجل لتوفير الحماية القانونية لأصحاب الحقوق، مما يستلزم وجود معاهدات دولية تحد من تلك الانتهاكات، وإصدار كل دولة قوانين متعلقة بالموضوع تعمل على حماية الملكية الفكرية؛ ومن أهم المعاهدات التي تم إبرامها في هذا الميدان معاهدة "برن" لحماية المصنفات الأدبية والفنية، والتي تم التوقيع عليها سنة 1971 بسويسرا، وكذا معاهدة "تريبس" والتي تم التوقيع عليها عام 1994، وقد تضمنت العديد من التدابير الهامة والإجراءات الفعالة لردع الاعتداءات على الملكية الفكرية، وتفرض هذه الاتفاقية على الدول اتخاذ العديد من التدابير المهمة، منها تمكين السلطات من إصدار الأوامر بشن حملات مفاجئة لضبط أدلة ارتكاب الجريمة، والتحفظ على أدوات ارتكاب الجرائم، وفرض عقوبات جزائية رادعة، وفي حالة تراخي الدولة العضو عن اتخاذ مثل تلك الإجراءات، أو إهمال في تطبيق قوانينها الوطنية، فإنها تعتبر مقصرة في أداء ما عليها، وتكون عرضة تبعا لذلك أن تتخذ ضدها العديد من الإجراءات العقابية من باقي الدول الأعضاء؛ من بين المعاهدات أيضا معاهدات "الويبو" الثلاث: معاهدة "الويبو" بشأن حق المؤلف، معاهدة "الويبو" بشأن الأداء والتسجيل الصوتي، ومعاهدة "الويبو" بشأن الحماية الدولية لحقوق المؤلف والحقوق المجاورة.[2]

على صعيد التعاون العربي، بدأت الدول العربية تستشعر ضرورة مواكبة الركب، وعدم البقاء في عزلة عن العالم، لذلك بادرت بإبرام الاتفاقية العربية لمكافحة جرائم تقنية المعلومات بالقاهرة في 2010/12/21، والتي صادقت عليها الجزائر بالمرسوم الرئاسي رقم 14-252 المؤرخ في 2014/9/08،[3] بالإضافة إلى القانون العربي الاسترشادي بشأن المعاملات والتجارة الإلكترونية، المعتمد بقرار من وزراء العدل العرب، رقم 812/د25، بتاريخ 2009/11/19، والقانون العربي

---

[1] المرجع نفسه، ص198.

[2] طارق فوزي الفقي، المرجع السابق، ص258.

أصدرت الجزائر المرسوم الرئاسي رقم 13-123 المؤرخ في 2013/04/03 يتضمن التصديق على معاهدة المنظمة العالمية للملكية الفكرية (الويبو) بشأن حق المؤلف، المعتمدة بجنيف بتاريخ 1996/12/30، ج ر عدد27 صادر في 2013/05/22، ص3.

[3] ج ر عدد 57 مؤرخ في 2014/9/28، ص4.

الاسترشادي للإثبات بالتقنيات الحديثة الذي اعتمده مجلس وزراء العدل العرب بقرار رقم 771/د24 في 2008/11/27.

على صعيد التشريعات الوطنية كانت السويد على رأس الدول التي سارعت إلى سن تشريعات خاصة بجرائم الانترنت، فقد أصدرت أول قانون سنة 1973، وهو قانون البيانات، الذي جرم الاحتيال الإلكتروني، وكذا الدخول غير المشروع على البيانات الإلكترونية، أو تحويلها، أو الحصول غير المشروع عليها، وتلتها بعض الدول في إصدار قوانين تجرم الجرائم الإلكترونية، بحيث أصدرت الولايات المتحدة قانونا خاصا بحماية أنظمة الحاسب الآلي عام 1985، ودعمته بآخر عام 1986، وأصدرت بريطانيا قانون مكافحة التزييف والتزوير عام 1981، وعززت كندا قانونها العقابي عام 1985 بإضافة نصوص خاصة بجرائم الحاسب والانترنت، أعطى صلاحيات أوسع لجهات التحقيق، وفي فرنسا فقد طور المشرع القوانين الخاصة لتتلاءم مع جرائم الحاسب الآلي والانترنت، فأصدر أول قانون عام 1988، الذي أضاف إلى قانون العقوبات جرائم الحاسب الآلي، وأضاف المشرع قواعد قانونية أخرى خاصة بالجرائم المعلوماتية، سواء من حيث الموضوع أو الإجراءات بموجب تعديل عام 1994،[1] بعدها بدأت تدخلات سريعة للمشرع في مجال المعلوماتية والانترنت، وخاصة قانون 575-2004 الصادر في 2004/6/21، المتعلق بالثقة في الاقتصاد الرقمي، وكذا قوانين 03 يناير 2008 و04 غشت 2008 التي عدلت قانون الاستهلاك على الانترنت، وكذلك قانون 12 جوان 2009 المتعلق ببث وحماية الاختراعات على الانترنت أو ما عرف بـ: "Hadopi 1 "، وكذلك قانون 28 أكتوبر 2009 المتعلق بالحماية الجزائية للملكية الأدبية والصناعية على الانترنت أو ما عرف بـ: "Hadopi 2"[2].

أما بالنسبة للتشريعات الداخلية للدول العربية، فإن بعض الدول العربية كانت سباقة لتعديل قوانينها أو إصدار قوانين جديدة، وكان أولها تونس التي أصدرت قانون التجارة الإلكترونية سنة 2000، وقانون عدد 5 لسنة 2004 المتعلق بالسلامة المعلوماتية، كما أن المملكة المغربية أصدرت القانون 03-07 المتمم لمجموعة القانون الجنائي فيما يخص الجرائم المتعلقة بنظم المعالجة الآلية للمعطيات، وكذا القانون 34.05 المتعلق بحقوق المؤلف والحقوق المجاورة، ومن الدول العربية الرائدة

[1] طارق فوزي الفقي، المرجع السابق، ص254.

[2] Jacques Larrieu, droit de l'internet, 2ème édition, éllipses édition, Paris 2010.

في مجال المعاملات الإلكترونية، دولة الإمارات العربية المتحدة التي أصدرت القانون الاتحادي رقم (2) لسنة 2006 المتعلق بمكافحة جرائم المعلومات،[1] أما المشرع المصري فقد أصدر القانون رقم 15 لسنة 2004 المتعلق بالتوقيع الإلكتروني.

أما المشرع الجزائري، فقد بدأ يهتم بالمعاملات الإلكترونية عامة، وظهر ذلك من خلال بعض النصوص القانونية منها المرسوم التنفيذي رقم 98-257 المؤرخ في 25 غشت 1998 والذي يضبط شروط وكيفيات إقامة خدمات الانترنت واستغلالها والقانون رقم 2000-03 المؤرخ في 05 غشت 2000، الذي يحدد القواعد العامة المتعلقة بالبريد وبالمواصلات السلكية واللاسلكية، أما التدخل الفعلي للمشرع الجزائري في الجانب الجزائي الخاص بالمعاملات الإلكترونية، فكان من خلال القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم لقانون العقوبات، والذي أضاف القسم السابع مكرر بعنوان: المساس بأنظمة المعالجة الآلية للمعطيات، والذي ضم المواد من 394 مكرر إلى 394 مكرر7 ووفر حماية جزائية موضوعية لمنظومة المعالجة الآلية للمعطيات، كما قام بتعديل قانون الإجراءات الجزائية بموجب القانون رقم 06-22 الصادر في 2006/09/20 والذي أدخل تغييرات إجرائية مهمة تتعلق بالجرائم المعلوماتية، وأصدر المشرع الجزائري أيضا القانون رقم 09-04 المؤرخ في 05 غشت 2009 والمتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، كما أصدر مؤخرا القانون 15-03 المتعلق بعصرنة العدالة، والقانون رقم 15-04 المؤرخ في الفاتح فبراير 2015 ويحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، كما صادقت الجزائر على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات التي وقعت عليها بالقاهرة سنة 2010، في انتظار قوانين أخرى تتعلق بالتجارة الإلكترونية بصورة مباشرة أو غير مباشرة.

[1] د. فؤاد بن صغير، الإجرام الإلكتروني، مطبعة النجاح الجديدة، الدار البيضاء، المملكة المغربية، ص4.

صعوبة موضوع البحث

إن المتصدي لموضوع الحماية الجزائية للتجارة الإلكترونية تعترض سبيله بعض الصعوبات من مثل:

– حداثة موضوع التجارة الإلكترونية خاصة بالنسبة لبلادنا، ولأدل على ذلك أن المشرع لا يزال في طور إصدار التشريعات المنظمة للموضوع.

– قلة المراجع المتخصصة التي تناولت الموضوع بعمق، وخاصة تلك المتعلقة بالجانب الجزائي، سواء أكان ذلك من الناحية الموضوعية أو من الناحية الإجرائية.

– تشعب موضوع التجارة الإلكترونية، بحيث يرتبط بمواضيع كثيرة كالتوقيع الإلكتروني، وبطاقات الوفاء والدفع، والإعلانات المضللة، وحماية المستهلك الإلكتروني، وحقوق الملكية الفكرية...وكل موضوع من هذه المواضيع يصلح لأن يشكل أطروحة دكتوراه، مما يجعل المتصدي لموضوع البحث في حيرة من أمره، خشية أن يقع في أحد المحظورين: الإطناب الممل أو الإيجاز المخل.

– يفرض موضوع الدراسة التطرق إلى أكثر من فرع من فروع القانون (مدني، تجاري، دولي...)، وإلى العودة باستمرار إلى القواعد العامة، كما يفرض الموضوع ضرورة الاطلاع على التشريعات المقارنة، خاصة تلك التي كان لها قصب السبق في هذا المجال.

– يفرض الموضوع الإلمام ببعض المصطلحات الفنية للتجارة الإلكترونية، والمعلوماتية بصفة عامة.

– ندرة الأحكام القضائية (ببلادنا) التي يمكن الاستئناس بها.

رغم هذه الصعوبات إلا أن الموضوع (شيق) ويستحق عناء البحث، ويفتح الباب على مصراعيه لمن يتصدى له، لطرق مواضيع أخرى مرتبطة به.

إشكالية البحث

إن حداثة موضوع التجارة الإلكترونية نسبيا، وعدم انتشارها ببلدان العالم الثالث بالقدر الذي تنتشر فيه في الدول المتقدمة، جعل بعض الدول ومنها الجزائر تتأخر نوعا ما عن مواكبة الركب من الناحية التشريعية، بيد أن التطورات السريعة في ميدان التعاملات الإلكترونية بدأت تفرض نفسها على الأرض، مما دفع مختلف الدول إلى سن القوانين المنظمة للتجارة الإلكترونية سواء من الناحية المدنية والتجارية أو من الناحية الجزائية، سواء ما تعلق منها بالجانب الموضوعي، أو الجانب الإجرائي.

لقد واجهت الكثير من الدول مشكلة الإجرام المعلوماتي، أو ما يسمى أيضا الجرائم المعلوماتية أو الإلكترونية، التي هددت المعاملات الإلكترونية وخاصة التجارة الإلكترونية، وللحد من هذا الإجرام، وإرجاع الثقة في الاقتصاد الإلكتروني أو الرقمي، كان لا بد من توفير حماية جزائية للتجارة الإلكترونية، غير أن السؤال المطروح: **هل يتم ذلك عن طريق سن قوانين جديدة بالكلية تتلاءم وطبيعة الجرائم الإلكترونية؟ أم تعدل القوانين الحالية لتستوعب هذه الجرائم الجديدة؟ أم أن القوانين الحالية يجوز تطبيقها على الجرائم الإلكترونية ولا يحتاج الأمر إلى إضافات أو تعديل؟**

كما أن الجرائم الواقعة على التجارة الإلكترونية متشعبة، فقد تمس الأموال كالنقود الإلكترونية أو بطاقات الوفاء، أو تمس خصوصية الأشخاص وبياناتهم التي لا يجوز الاطلاع عليها، أو تمس الأسرار التجارية الخاصة بالشركات، كما يمكن أن يتعرض المستهلك إلى الغش والخداع عبر التجارة الإلكترونية، أو يتعرض إلى بعض الجرائم التقليدية كالنصب وخيانة الأمانة؛ كما أن الموقع الإلكتروني ذاته في حاجة إلى حماية جزائية، سواء فيما يتعلق بمحتواه، أو بعنوانه، مما يثير تساؤلات الفقه حول جدوى القوانين التقليدية في توفير الحماية المطلوبة، غير أن الدول التي لا تمتلك قوانين خاصة مضطرة لتفسير قوانينها التقليدية تفسيرا واسعا كي تستوعب الجرائم المستحدثة، وهذا الأمر يراه البعض يتعارض مع مبدأ المشروعية الجنائية الذي يتفرع عنه مبدأ التفسير الضيق للقانون الجزائي، وكذا قاعدة عدم جواز القياس في القانون الجزائي، مما يستدعي تدخلا سريعا من المشرع لسد الخلل.

وإذا كانت الجوانب المتعلقة بتوفير حماية جزائية موضوعية للتجارة الإلكترونية تثير الكثير من التساؤلات، فإن المسائل الإجرائية المتعلقة بهذه التجارة أكثر إثارة للجدل، حيث طرح الفقه

المقارن العديد من التساؤلات بهذا الصدد، منها: هل النصوص الإجرائية التقليدية كافية لمكافحة الجرائم الواقعة على التجارة الإلكترونية؟ أم لا بد من تدعيمها بنصوص جديدة؟ أم يجب استصدار نصوص إجرائية خاصة بهذا النوع من الجرائم؟

غالبية الفقه يرى أن الطبيعة الخاصة للجرائم الإلكترونية، تجعل من الصعب جدا كشفها بالقواعد الإجرائية التقليدية، لذا فإن العديد من الدول عدلت قوانينها الجزائية لمحاربة هذا النوع من الجرائم، غير أن السؤال المطروح: **إلى أي مدى وفقت في تعديلاتها هذه؟ وهل استطاعت أن تحقق التوازن بين حق الأفراد في الخصوصية ومصلحة المجتمع في متابعة المذنبين؟ وهل تمتلك الدول من الكفاءات الفنية اللازمة لمجابهة هذه الجرائم؟ وما هي أبرز المشاكل التي يمكن مواجهتها عند البحث عن الأدلة الإلكترونية سواء في مرحلة البحث والتحري أو في مرحلة التحقيق والمحاكمة؟**

تعتبر الجرائم الواقعة على التجارة الإلكترونية جرائم عالمية، لذلك فهي تثير مشكلة القانون الواجب التطبيق، والمحكمة المختصة، وكذا مسألة التعاون الدولي الذي يعتمد في الغالب على إرادة الدول السياسية في التعاون، إذ أن بعض جوانبه قد تمس بسيادة الدول، والسؤال المطروح: **إلى أي مدى يسهم التعاون الدولي في محاربة الجرائم الواقعة على التجارة الإلكترونية؟ وما هي سبل تعزيزه؟ وما هي المعوقات التي تعترضه؟ وكيف يمكن التغلب عليها؟** خاصة وأن الكثير من الدول – الضعيفة خاصة- تخشى أن يتخذ من موضوع محاربة الجرائم العالمية بصفة عامة، والجرائم المتعلقة بالتجارة الإلكترونية بصفة خاصة، ذريعة للتدخل في سياساتها الداخلية، والنيل من سيادتها أو الانتقاص منها.

بناء على كل ما تقدم، يبدو أن الإشكالية الرئيسة لهذا الموضوع تتمثل في الإجابة عن السؤال التالي: **إلى أي مدى تستطيع القوانين الجزائية الموضوعية والإجرائية بشكلها الحالي أو بعد تعديلها وإتمامها إضفاء الحماية الجزائية الكافية على التجارة الإلكترونية، دون المساس بالحقوق الشخصية للأفراد؟ أو بسيادة الدول؟**

خطة البحث

لمعالجة هذا الموضوع تم تقسيم البحث إلى فصل تمهيدي وبابين، حيث تطرق الفصل التمهيدي إلى ماهية التجارة الإلكترونية قصد إلقاء الضوء على بعض مفاهيمها، وبعض جوانبها لتكون مدخلا للدراسة، كما تناول مفهوم الجرائم المعلوماتية والمجرم المعلوماتي، باعتبار أن هناك تلازما بين التجارة الإلكترونية والجرائم المعلوماتية، بحيث تعتبر هذه الأخيرة الخطر الكبير الذي يهدد التجارة الإلكترونية، ويقوض ثقة المتعاملين فيها، والذي تعمل التشريعات المختلفة على التصدي له، وتناول الباب الأول الحماية الجزائية الموضوعية للتجارة الإلكترونية، وحاول من خلال الفصل الأول التطرق إلى موضوع مواقع التجارة الإلكترونية وضرورة حمايتها عن طريق تجريم الاعتداء على نظم المعالجة الآلية للمعطيات، وكذلك حمايتها عن طريق قوانين الملكية الفكرية، وأثار الكثير من النقاط سواء ما تعلق منها بالدخول والبقاء غير المشروعين إلى مواقع التجارة الإلكترونية، أو جنحة التقليد، أو النزاعات بين أسماء النطاق أو العناوين الإلكترونية والعلامات التجارية، أما الفصل الثاني فتطرق إلى حماية المستهلك الإلكتروني من بعض الجرائم الإلكترونية التقليدية والمستحدثة، وتم التطرق في هذا الفصل إلى نقاط كثيرة منها بطاقات الائتمان، التوقيع الإلكتروني، الإعلانات الكاذبة أو الخادعة عبر الإنترنت، مسؤولية مقدمي الخدمات وغيرها من المواضيع، أما الباب الثاني من البحث فاهتم بالحماية الجزائية الإجرائية للتجارة الإلكترونية من خلال فصلين، تناول الأول الحماية الجزائية الإجرائية في التشريعات الوطنية، من خلال التطرق إلى جملة من المواضيع تتعلق بإجراءات التحري والتحقيق والمحاكمة في جرائم التجارة الإلكترونية، والخصوصية التي تنفرد بها هذه الجرائم عن غيرها، ومجهودات التشريعات المقارنة للتعامل الفعال معها، دون المساس بمبدأ المشروعية، أما الفصل الثاني فتطرق إلى التعاون الدولي في مجال مكافحة جرائم التجارة الإلكترونية، وأبرز ضرورته كون الجرائم الواقعة على التجارة الإلكترونية عالمية في الغالب، يلزم لمجابهتها تكاتف الجهود، كما أماط اللثام عن الصعوبات التي تعترض سبيل هذا التعاون، وأكثرها فنية وسياسية، وحاول إعطاء بعض المقترحات قصد التغلب عليها.

الفصل التمهيدي: التجارة الإلكترونية والجرائم المعلوماتية

يتناول هذا الفصل موضوع ماهية التجارة الإلكترونية (المبحث الأول)، ثم يتعرض إلى الجرائم المعلوماتية (المبحث الثاني)، باعتبار أن أكبر خطر يتهدد أمن وسلامة التجارة الإلكترونية هو الجرائم المعلوماتية.

المبحث الأول: ماهية التجارة الإلكترونية

يتناول هذا المبحث جملة من النقاط، أبرزها إعطاء تعريف للتجارة الالكترونية، يُعتمد عليه فيما بعد عند التطرق إلى الحماية الجزائية للتجارة الالكترونية، كما يهتم أيضا بتبيان التطور الذي عرفته هذه التجارة، بالإضافة إلى إبراز أهم خصائصها وأنواعها، ووسائلها...

يقسم هذا المبحث إلى مطلبين، يتناول الأول مفهوم التجارة الالكترونية ومميزاتها، أما المطلب الثاني فيهتم بواقع وآفاق هذه التجارة.

المطلب الأول: مفهوم التجارة الالكترونية ومميزاتها.

يقسم هذا المطلب إلى فرعين، يتناول الأول مفهوم التجارة الالكترونية، أما الفرع الثاني فيهتم بتبيان أهم مميزات هذه التجارة.

الفرع الأول:مفهوم التجارة لإلكترونية.

يحاول هذا الفرع إعطاء تعريف للتجارة الالكترونية، وإبراز مراحل تطورها.

أولا: تعريف التجارة الإلكترونية

من حيث اللغة ينقسم مصطلح التجارة الإلكترونية إلى كلمتين:

التجارة: وتعني ممارسة البيع والشراء، وهي حرفة التاجر الذي يمارس الأعمال التجارية على وجه الاحتراف.[1]

[1] فهد بن سيف بن راشد الحوسني، جرائم التجارة الالكترونية ووسائل مواجهتها مع التطبيق على سلطنة عمان، رسالة مقدمة لنيل درجة دكتوراه في علوم الشرطة، أكاديمية الشرطة، كلية الدراسات العليا، القاهرة 2007، ص3.

الإلكترونية: نسبة إلى الإلكترون وهو أحد مكونات الذرة، وهو جسم متناه في الصغر، وتنسب إلى الإلكترون كل الأجهزة والوسائل التي تؤدي وظائفها من خلال حركة الإلكترون، تحت تأثير مجال كهربائي أو مغناطيسي.

وقد عرف مجمع اللغة العربية بمصر الإلكترون بأنه: "دقيقة ذات شحنة كهربائية سالبة، شحنتها هي الجزء الذي لا يتجزأ من الكهربائية". [1]

من تجميع الكلمتين نستنتج أن التجارة الإلكترونية يقصد بها تلك التجارة التي تقوم أساسا على وسائل تقنية حديثة؛ بمعنى أن هذه التجارة تتم بوسائل إلكترونية كالانترنت والفاكس والهاتف المحمول وغيرها.

بالنظر إلى التعريف اللغوي، فإنه يبدو للوهلة الأولى من السهل إعطاء تعريف قانوني للتجارة الإلكترونية، ولكن الأمر ليس بهذه السهولة، حيث أن التجارة الإلكترونية هي مجال جديد وشامل يتضمن مجموعة واسعة من العلوم التقنية والإدارية والقانونية مثل الحاسوب، وتقنية المعلومات والتسويق والمالية، والاقتصاد، ونظم المعلومات الإدارية والمحاسبة، وإدارة الأعمال، والقانون وغيرها.[2] ورغم ذلك يمكن القول أن أي تعريف للتجارة الالكترونية ينبغي أن يتضمن ثلاثة عناصر أساسية وهي:[3]

- فكرة النشاط التجاري، ذلك أن هذه التجارة ما هي إلا عمل أو مشروع تجاري.
- عدم اعتماد التجارة الالكترونية على الدعامات الورقية في مختلف المعاملات التجارية.
- فكرة التدويل أو العولمة المقترنة بالتكنولوجيا المتقدمة، وتثير الكثير من المسائل القانونية المتعلقة بالقانون الواجب التطبيق والمحكمة المختصة.

وهناك من يعرف التجارة بأنها مجموع النشاطات المنظمة والممتدة على الشبكات المفتوحة (بيع شراء إعلان) وشتى الأعمال التجارية التي تعمل على تبادل القيم بين الطرفين. والشبكات المفتوحة هي تلك التي يجوز استخدامها من طرف الجميع دون الحاجة إلى اتباع أي بروتوكولات معينة. محمد إبراهيم أبو الهيجاء، عقود التجارة الالكترونية، دار الثقافة، عمان، الأردن 2005، ص25.

[1] إبراهيم بن سطم بن خلف العنزي،التوقيع الإلكتروني وحمايته الجنائية، أطروحة لنيل درجة دكتوراه في الفلسفة، تخصص العلوم الأمنية، الرياض 2009، ص37.

[2] محمد نور برهان وعز الدين خطاب، التجارة الالكترونية، الشركة العربية المتحدة للتسويق والتوريدات، القاهرة، مصر 2009، ص11.

[3] عبد الفتاح بيومي حجازي، التجارة الالكترونية وحمايتها القانونية، الكتاب الأول، نظام التجارة الالكترونية وحمايتها المدنية، دار الكتب القانونية، المحلة الكبرى، مصر 2007.ص22.

وقد تعددت الجهات التي اهتمت بالتجارة الالكترونية، وأبرزها الأمم المتحدة، والوثائق الأوربية، والقوانين المختلفة، بالإضافة إلى الفقه.

1- : تعريف لجنة الأمم المتحدة للتجارة الالكترونية.

في البدء كان هناك مصطلح تبادل المعطيات المعلوماتية (Edi)[1] وقد تطور في النظام الأمريكي، ولكن الأمم المتحدة استخدمت اصطلاحا أكثر عمومية وتطورا من هذا المصطلح وهو (Edifact)[2] ويعني تبادل معطيات المعلوماتية في مجالات الإدارة والتجارة والنقل.

بتاريخ 16 ديسمبر 1996 وافقت لجنة الأمم المتحدة للقانون التجاري الدولي على نموذج لمشروع قانون موحد للتجارة الإلكترونية،[3] غير أنه خلا من إعطاء تعريف لها، مكتفيا بتعريف "التبادل الالكتروني للبيانات" والتي تشمل التجارة الالكترونية، وورد فيه بأن تبادل البيانات الالكترونية هو"نقل المعلومات إلكترونيا من حاسوب إلى حاسوب آخر باستخدام معيار متفق عليه لتكوين المعلومات".[4]

وحسب الدليل التشريعي لهذا القانون النموذجي، فإن اللجنة واضعة القانون قد تعمدت عدم تحديد مفهوم التجارة الالكترونية، وإعطاء مصطلح أوسع "التبادل الالكتروني للبيانات"، يشمل مجموعة موسعة من استخدام التبادل الالكتروني للبيانات المتصلة بالتجارة، كالإبلاغ عن طريق التبادل الالكتروني للبيانات، وإرسال نص لا يراعي شكلا محددا بالوسائل الالكترونية عن طريق الانترنت مثلا، أو استخدام تقنيات مثل التلكس والنسخ البرقي.[5]

2- تعريف التجارة الالكترونية في الوثائق الأوربية

عرف توجيه البرلمان والمجلس الأوربي رقم 7/97 الصادر في 20 مايو 1997 في شأن حماية المستهلكين في مجال العقود عن بعد في المادة الثانية العقد عن بعد بأنه كل عقد يتعلق بالبضائع أو

---

[1] Echange de données informatisées

[2] Echange de données informatisées pour l'administration, le commerce et le transport.

[3] قانون نموذجي تحتذي به الدول في سن تشريعاتها.

[4] بيومي حجازي، المرجع السابق، ص24، ويراجع أيضا نص م2/ب من قانون التجارة الالكترونية (الأونسيترال).

[5] وائل أنور بندق، قانون التجارة الالكترونية (قواعد الأونسيترال ودليلها التشريعي)، مكتبة الوفاء القانونية، الإسكندرية، مصر 2009. ص33.

الخدمات أبرم بين مورد ومستهلك في نطاق نظام لبيع أو لتقديم خدمات عن بعد، نظمه المورد الذي يستخدم، لهذا العقد، فقط، تقنية أو أكثر للاتصال عن بعد لإبرام العقد وتنفيذه.[1]

وعرف التوجيه ذاته تقنية الاتصال عن بعد بأنها كل وسيلة دون وجود مادي ولحظي للمورد والمستهلك، يمكن أن تستخدم لإبرام العقد بين طرفيه.[2]

وقد بين الملحق الأول للتوجيه تقنيات الاتصال، وذكرها على سبيل المثال،[3] ليترك المجال لأية وسيلة أخرى يتحقق بها الاتصال عن بعد، ودون وجود مادي ولحظي لطرفي العقد.[4]

والملاحظ حول هذا التوجيه هو إعطاء الحق للمستهلك في إرجاع السلعة أو رفض الخدمة خلال مدة معينة من تاريخ العقد، وهو حق لا يجوز إنكاره على المستهلك من طرف مقدم الخدمة.[5]

وعرف توجيه البرلمان والمجلس الأوربي رقم 31/2000 الصادر في 08 جويلية 2000 بشأن بعض الجوانب القانونية لخدمات شركة المعلومات وبصفة خاصة التجارة الالكترونية في السوق المحلية (توجيه التجارة الالكترونية) في المادة الثانية الاتصال التجاري بأنه كل شكل من أشكال الاتصال يستهدف تسويق، بصورة مباشرة أو غير مباشرة، بضائع أو خدمات أو صورة مشروع أو منظمة أو شخص يباشر نشاطا تجاريا أو صناعيا أو حرفيا أو يقوم بمهنة منظمة.[6]

وحث التوجيه الدول الأعضاء على أن تسمح أنظمتها القانونية بإبرام العقود بالطرق الالكترونية، وعدم عرقلتها أو الحد من فاعليتها لمجرد أنها تتم بالطرق الالكترونية.[7]

---

[1] مدحت عبد الحليم رمضان، الحماية الجنائية للتجارة الالكترونية، دراسة مقارنة، دار النهضة العربية، القاهرة، مصر2012.ص13.

[2] المرجع نفسه، ص14.

[3] ومنها: المطبوعات غير المعنونة والمعنونة والخطابات الموحدة والدعاية مع نموذج الطلب، والكتالوجات والتلفون مع تدخل إنساني والتلفون دون تدخل إنساني، والتلفون المرئي (الفيزيوفون) والفيديو تكست، والميكرو كمبيوتر والمراسلات الالكترونية وأجهزة التصوير، والتلفزيون. المرجع نفسه، ص14.

[4] عبد الفتاح بيومي حجازي، المرجع السابق، هامش ص35.

[5] المرجع نفسه، ص37.

[6] مدحت عبد الحليم رمضان، المرجع السابق، ص15.

[7] مدحت عبد الحليم رمضان، المرجع السابق، ص15.

3- تعريف التجارة الالكترونية في القوانين المقارنة

في فرنسا، عرفت مجموعة العمل المشكلة برئاسة وزير الاقتصاد الفرنسي سنة 1998 التجارة الالكترونية بأنها "مجموعة المعاملات الرقمية المرتبطة بأنشطة تجارية، بين المشروعات ببعضها البعض، وبين المشروعات والأفراد، وبين المشروعات والإدارة".[1]

يعد هذا التعريف واسعا، فهو من جهة ينصرف إلى ما بين المشروعات بعضها البعض، ولذلك يشمل علاقات البنوك بعضها ببعض، وعلاقات الشركات التجارية بعضها ببعض، أيا كان نشاطها، ودورها. ومن جهة ثانية يشمل التعريف علاقات الشركات والأفراد. ومن جهة ثالثة ينصرف هذا التعريف ليشمل كافة عقود الإدارة المبرمة مع المشروعات (الشركات).[2]

أصدر المشرع الفرنسي القانون رقم 2000/230، في شأن قانون الإثبات والمتعلق بالتوقيع الإلكتروني، ولكنه لم يتضمن تعريفا محددا بشأن التجارة الإلكترونية، ولم يتم تعريفها إلا سنة 2004، بفضل قانون 21 جوان 2004 المتعلق بالثقة في الاقتصاد الرقمي المعروف اختصارا ب LCEN، في المادة 14 الفقرة الأولى، كما يلي: "التجارة الإلكترونية تعني النشاط الاقتصادي الذي عن طريقه، يقترح شخص أو يضمن عن بعد وبوسيلة إلكترونية التزويد بالسلع والخدمات".[3]

في إيطاليا، صدر قرار بقانون سنة 1999 في شأن التجارة الالكترونية قنن اتجاه البرلمان والمجلس الأوربي رقم 7/97 المتعلق بحماية المستهلكين في مجال العقود عن بعد.[4]

أما عربيا فقد كانت تونس سباقة في إصدار قانون التجارة الالكترونية، وكان ذلك في 09 أوت 2000، وأورد القانون في الفصل الثاني منه تعريفا لكل من المبادلات التجارية، والتجارة

---

[1] المرجع نفسه، ص12.

[2] بيومي حجازي، المرجع السابق، ص26.

[3] Le commerce électronique désigne « l'activité économique par laquelle une personne propose ou assure à distance et par voie électronique la fourniture de biens ou se services ».
Christiane Féral-Schuhl, cyberdroit, le droit à l'épreuve de l'internet, 5ème édition, Dalloz, Paris 2008/2009, p245.

[4] ويعتبر جانب من الفقه الإيطالي أن التجارة الالكترونية تختلف عن البيع عن بعد، حيث أن المستهلك في التجارة الالكترونية لا يقف موقفا سلبيا كما هو شأن المستهلك في البيع عن بعد، بل يسهم إيجابا وبشكل مباشر في إعداد العقد عن طريق البحث عن الكتالوجات مباشرة، وإجاباته على الدعوة للتعاقد من قبل التجار. لكن جانبا من الفقه الإيطالي لا يرى اختلافا كبيرا بين التجارة الالكترونية والبيع عن بعد، إذا وضع في الحسبان أن المستهلك لا يطلع مباشرة على المال محل العقد. مدحت عبد الحليم رمضان، المرجع السابق، ص16.

الالكترونية، حيث عرف المبادلات التجارية بأنها" المبادلات التي تتم باستعمال الوثائق الالكترونية"، وعرف التجارة الالكترونية بأنها "العمليات التجارية التي تتم عبر المبادلات الالكترونية".[1]

أما مشروع قانون التجارة الالكترونية المصري فعرف في مادته الأولى التجارة الالكترونية بأنها:"كل معاملة تجارية تتم عن بعد باستخدام وسيلة الكترونية".[2]

والملاحظ حول التعريف أنه لم يحدد الوسيلة الالكترونية التي تتم بها التجارة، وهو أمر يحسب له، لأن الوسائل التقنية في تطور مستمر.[3]

وعرفت المادة الثانية من قانون التجارة الالكترونية رقم 2 لإمارة دبي لسنة 2002 التجارة الالكترونية بأنها"المعاملات التجارية التي تتم بواسطة المراسلات الالكترونية".[4]

وتكمن أهمية التعريفات التي يضعها المشرع في أمرين: الأول أنها تضع معنى محددا لمصطلحات تترتب على استخدامها آثار قانونية، والثاني أن هذه التعريفات تزيل اللبس الذي قد يحدث في فروع قانونية مستحدثة ليس لها مصادر أخرى يمكن الرجوع إليها طلبا للتفسير.[5]

4- تعريف الفقه للتجارة الالكترونية

كأي موضوع جديد، يسترعي اهتمام الباحثين، فإن التجارة الالكترونية وجدت اهتماما كبيرا من قبل الفقهاء، وقيل بشأنها تعريفات كثيرة، فقد عرفت بأنها:" تنفيذ وإدارة الأنشطة التجارية المتعلقة بالبضاعة والخدمات بواسطة المعطيات عبر شبكة الانترنت".[6]

وعرفت بأنها: "جميع العمليات التجارية التي تتم ضمن وسيط إلكتروني هو الانترنت".[7]

---

[1] بيومي حجازي، المرجع السابق، ص41.

[2] المرجع نفسه، ص39.

[3] المرجع نفسه، ص40.

[4] بيومي حجازي، التجارة الالكترونية في القانون العربي النموذجي لمكافحة جرائم الكمبيوتر والانترنت، دار الفكر الجامعي، الإسكندرية، مصر 2006، ص50.

[5] المرجع نفسه، ص51.

[6] سليم سعداوي، عقود التجارة الالكترونية. دراسة مقارنة، دار الخلدونية. القبة الجزائر 2008، ص11.

[7] محمد إبراهيم أبو الهيجاء، المرجع السابق، ص25.

الملاحظ أن هذين التعريفين قد ربطا بين التجارة الالكترونية والانترنت، والصحيح أن التجارة الالكترونية لا تتم فقط عبر الانترنت، رغم كونها الوسيلة الأكثر شيوعا واستعمالا، وإنما تتم أيضا بوسائل أخرى؛ فمنذ سنوات عديدة خلت استعملت شبكات من نوع (Edi)، كما أن عمليات التجارة الالكترونية يمكن أن تتم بواسطة الهواتف النقالة (commerce Mobile)، وفي فرنسا ومنذ الثمانينيات استعمل جهاز المينتال في هذا النوع من المبادلات التجارية.[1]

ومن بين التعريفات الواردة بشأن التجارة الالكترونية تعريف الجمعية الفرنسية "للتليماتيك والميلتيميديا"، ومفاده بأنها مجموعة المعاملات التجارية التي يتم الشراء فيها عن طريق وسائل الاتصال. وبالتالي فإن التجارة الالكترونية تشمل عملية تلقي الطلب وكذلك الشراء مع السداد، وتتعلق بصورة أكبر بالعمليات المتعلقة بشراء السلع من تلك المتعلقة بالخدمات، سواء اتخذت الأخيرة شكل المعلومات أو شكل الألعاب.[2]

وحاول جانب من الفقه المصري تعريف التجارة الالكترونية، فعرفها بأنها:"تنفيذ بعض أو كل المعاملات التجارية في السلع والخدمات التي تتم بين مشروع تجاري وآخر، أو بين مشروع تجاري ومستهلك، وذلك باستخدام تكنولوجيا المعلومات والاتصال".[3]

وعرفها جانب آخر من الفقه المصري بأنها: "عملية البيع والشراء عبر الشبكات الالكترونية على المستويين السلعي والخدمي، بجانب المعلومات وبرامج الكمبيوتر، وأي أنشطة أخرى تساعد على الممارسات التجارية".[4]

والملاحظ في هذا التعريف أنه أضاف موضوعات أخرى يمكن أن تكون محلا للتجارة الالكترونية وخاصة برامج النظم والبيانات والمعلومات.[5]

---

[1] الموقع الالكتروني: http://fr.wikipedia.org/wiki/Commerce_%C3%A9lectronique تاريخ الولوج: 2012/05/06 على الساعة 15.

[2] مدحت عبد الحليم رمضان، المرجع السابق، ص18.

[3] بيومي حجازي، المرجع السابق، ص54.

[4] المرجع نفسه، ص54.

[5] المرجع نفسه، ص54.

وعرفت التجارة الالكترونية بأنها "مجموعة متكاملة من عمليات عقد الصفقات وتأسيس الروابط التجارية وتوزيع وتسويق وبيع المنتجات بوسائل إلكترونية".[1]

وخلاصة القول نؤيد ما ذهب إليه جانب من الفقه المصري بأن التجارة الالكترونية ما هي بداهة إلا نوع من التجارة، تتم بوسائل إلكترونية. هذه الوسائل التي لا تقتصر فقط على الانترنت، بل تتعداها إلى كل الوسائل الالكترونية التي يمكن أن تتم بها التجارة الالكترونية، تعطي لهذه التجارة خصائص ومميزات فريدة من نوعها.

ثانيا: مراحل تطور وظهور التجارة الالكترونية

التجارة الالكترونية ليست حديثة تماما، إذ ترجع جذورها إلى منتصف الأربعينيات، حيث تم اكتشاف أول كمبيوتر، خلال الحرب العالمية الثانية، ونتيجة لجو السرية الذي ميز هذه الحقبة من الزمن لم يعرف الآباء الحقيقيون للكمبيوتر الحديث.[2] وفي أواخر الخمسينيات سخرت الشركات الكبرى الحاسبات لإيجاد نوع من التكامل نصف الآلي بينها وبين الموردين الرئيسيين لها، وفي منتصف الستينيات بدأت مرحلة التبادل الالكتروني للبيانات باستخدام الشبكات الخاصة.[3] وبعد ذلك قامت مجموعة من الشركات الانجليزية بإنشاء أول شبكة إلكترونية لخدمات نقل وتبادل الوثائق، ثم إنشاء شبكات القيمة المضافة التي كان لها دور كبير في تحقيق الارتباط بين الشركات التجارية.[4]

ونتيجة للتطورات السريعة التي فرضتها العولمة الاقتصادية، وما واكبها من ظهور التقنيات الحديثة وخاصة الانترنت، وانتشار الشركات متعددة الجنسيات، وزيادة معدلات انتقال رؤوس الأموال بين الدول، والاستثمارات الأجنبية المباشرة، ظهرت نماذج وتطبيقات الأعمال الالكترونية التي سهلت تلبية احتياجات العملاء في الوقت المناسب، وبجودة وسعر ملائمين. أدى هذا الأمر إلى إدخال العمليات الالكترونية في جميع الأعمال التجارية، وتبني نظام الإدارة المفتوح في جميع الوظائف، حيث تتأثر كل وظيفة بمنظمة الأعمال وتتجاوب مع التغيرات والمؤثرات الداخلية والخارجية. وتعتبر الانترنت

---

[1] محمد الصيرفي، التجارة الالكترونية، مؤسسة حورس الدولية، الإسكندرية، مصر 2005، ص147.

[2] محمد سعيد أحمد إسماعيل، أساليب الحماية القانونية لمعاملات التجارة الالكترونية، دراسة مقارنة، منشورات الحلبي الحقوقية، بيروت، لبنان 2009، ص30.

[3] محمد سعيد أحمد إسماعيل، المرجع السابق، ص31.

[4] المرجع نفسه، ص32.

أهم حدث تكنولوجي أثر على عالم الاقتصاد في العقد الأول من هذه الألفية، دون إغفال الدور الرئيس الذي لعبته الأقمار الصناعية في هذا المجال، مما أدى إلى انتشار القنوات الفضائية واشتداد المنافسة التجارية.[1]

وساهم انتعاش التجارة الدولية في الأجهزة الالكترونية، في انتشار هذه الأجهزة بين المستهلكين، مما أتاح لهم فرصة استغلالها في أغراض مختلفة من بينها التجارة الدولية. وقد لمس المستهلك نتائج وآثار التقدم التكنولوجي على حياته الشخصية والعملية. وبتقدم التكنولوجيا تقدمت الصناعة ووسائل الاتصال، وهو ما أثر إيجابا على حجم التبادل التجاري بواسطة هذه الوسائل الحديثة.[2]

ولضمان هذه الإيجابيات، وحماية لأطراف هذه التجارة ظهرت الحاجة إلى وضع تنظيم قانوني يحكمها من حيث كيفية التعاقد، وحفظ حقوق المتعاقدين وإثباتها، وكذلك الحماية الجزائية لهذه التجارة والمتعاملين بها،[3] ضمانا للثقة التي يجب أن تسود المعاملات التجارية.

الفرع الثاني: مميزات التجارة الالكترونية

يتم التعرض أولا إلى أنواع وخصائص التجارة الالكترونية)، ثم إلى الوسائل التي تعتمد عليها هذه التجارة.

أولا: أنواع وخصائص التجارة الالكترونية

يتم التطرق أولا إلى أنواع التجارة الالكترونية ثم تبيان أهم خصائصها والتي تميزها عن التجارة التقليدية.

1- أنواع وصور التجارة الالكترونية

التجارة الالكترونية نوعان، فقد تكون الصفقات التجارية المبرمة إلكترونية بحتة، مثل تبادل المعلومات أو منتجات الكمبيوتر، أو الكتب الالكترونية، أو المنتجات الفنية، حيث يتم تسليم هذه السلع أو الخدمات رقميا للمشتري عن طريق تحميلها من الشبكة إلى جهاز المشتري، وقد تكون

[1] محمد الصيرفي، المرجع السابق، ص149.

[2] بيومي حجازي، المرجع السابق، ص12.

[3] بيومي حجازي، المرجع السابق، ص13.

الصفقات التجارية المبرمة جزئية (تجارة إلكترونية جزئية)، وذلك عندما يكون أحد العناصر رقمي وعناصر أخرى مادية، كأن يقوم العميل بشراء كتاب من موقع على الانترنت، ويطلب من الشركة إرسال الكتاب إلى محل إقامته عن طريق البريد العادي.[1]

أما أشكال أو صور التجارة الالكترونية فهي:

أ- التجارة الالكترونية بين وحدة أعمال ووحدة أعمال (business to business) "B2B" تقوم وحدة الأعمال بتقديم طلبات الشراء إلى وحدات الأعمال الأخرى، ويتم تبادل البيانات والمعلومات حتى يتم التوصل إلى اتفاق بينهما، وعندها يبرم عقد إلكتروني لتوريد السلع أو الخدمات، ويتم تسليم الفواتير وتسديد المستحقات إلكترونيا، أما التسليم فقد يكون إلكترونيا أو ماديا حسب الاتفاق، أو طبيعة السلع والخدمات.

وهذا النوع هو الأكثر شيوعا لمعاملات التجارة الالكترونية في الوقت الراهن، إذ يمثل نحو 80% من إيراداتها. ومن أمثلة التجارة الالكترونية لمشروعات الأعمال فيما بينها المتاجرة عبر الانترنت في مختلف السلع، كما تعتبر التجارة الدولية النموذج الأمثل لهذا النوع من أعمال التجارة الالكترونية.[2]

ب- التجارة الالكترونية بين وحدة أعمال ومستهلك "B2C" مع ظهور الأسواق الالكترونية على شبكة الانترنت وانتشار المعلومات وتكنولوجيا المعلومات، بدأت هذه التجارة في الازدهار، إذ يتجول الزائرون عادة بين مختلف المتاجر الموجودة في المجمعات الالكترونية للتعرف على السلع والمنتجات والخدمات المعروضة، ويقومون بالتسوق مباشرة، ويسددون بطرق إلكترونية كالشيكات الالكترونية وبطاقات الائتمان.[3]

[1] محمد سعيد أحمد إسماعيل، المرجع السابق، ص40.

[2] محمد سعيد أحمد إسماعيل، المرجع السابق، ص41.

[3] المرجع نفسه، ص42.

ت- التجارة الالكترونية بين مستهلك ومستهلك آخر "C2C" كالبيع والشراء الذي يتم بين مستهلك ومستهلك آخر عبر شبكة الانترنت، ومثال ذلك مواقع المزادات المختلفة المتواجدة على الانترنت التي يستطيع من خلالها الأفراد البيع أو الشراء مباشرة.[1]

ث- التجارة الالكترونية بين مستهلك ووحدة أعمال "C2B" ويمارس هذه العملية في الغالب الوسطاء الإلكترونيون الذين يعرضون خدماتهم على الانترنت، وقد يقدمون معلومات أو خدمات أو منتجات إلى الشركات.[2]

ج- التجارة الالكترونية والأعمال الداخلية: ويتضمن كل الأنشطة التنظيمية الداخلية والتي عادة ما تكون على شبكة الأنترانت، والتي تحاط بما يسمى الجدار الناري.[3]

ح- التجارة الالكترونية بين المستهلك والحكومة "C2G" وهو ما يصطلح عليه الحكومة الالكترونية، حيث يستطيع المواطن إجراء معاملاته عن طريق الانترنت، وفي هذه الحالة ليست كل المعاملات التي يجريها المستهلك مع الحكومة تجارية.[4]

خ- التجارة الالكترونية بين الشركات والحكومة "B2G" كالتفاعلات بين الشركات والحكومة والتي تدخل في الإطار التجاري كعمليات الشراء التي تقوم بها الحكومة من الشركات التجارية.[5]

2- خصائص التجارة الالكترونية

إن إبراز أهم ما تتميز به التجارة الالكترونية لا يتأتى جليا إلا بمقارنتها مع التجارة التقليدية.

لقد أصبحت التجارة التقليدية تعاني العديد من جوانب الضعف، كطول الفترة التي تستغرقها العملية التجارية، والجهد الكبير المبذول لإتمامها، وتعدد أطرافها من مخازن ومبيعات وأدوات شحن، وصعوبة عملية الرقابة والإشراف عليها، وكثرة العنصر البشري المشترك فيها مما قد يؤدي إلى

---

[1] المرجع نفسه، ص43.

[2] المرجع نفسه، ص44.

[3] المرجع نفسه، ص44.

[4] سليم سعداوي، المرجع السابق، ص155.

[5] المرجع نفسه، ص155.

كثرة الأخطاء، وزيادة المشكلات المتعلقة بإدارة هذا العنصر البشري، وكذا صعوبة تبادل المعلومات بسبب كثرة العمليات والأطراف المشتركة في التجارة التقليدية.[1]

أما التجارة الالكترونية فإن مزاياها عديدة، وأهمها: زيادة القدرة التنافسية بين المشروعات، قلة تكلفة عقد الصفقات، تشجيع المشروعات الصغيرة والمتوسطة، السرعة والفاعلية،[2] وتتميز هذه التجارة بأن منتجاتها غير ملموسة، كما أن البائع لا يلتقي مباشرة مع المشتري، و لا يشترط وجود سوق فعلية، فالسوق في هذه التجارة افتراضية، كما أن عملية التبادل لا تستغرق وقتا طويلا، إذ قد تتم في دقائق معدودات أو أقل، كما أن وسائل السداد مختلفة عن وسائل السداد في التجارة التقليدية، إذ تستعمل النقود الرقمية وبطاقات الائتمان والشيكات الالكترونية.[3]

ثانيا: وسائل التجارة الالكترونية.

تعالج هذه النقطة من خلال التطرق إلى وسائل إبرام العقود الالكترونية، والتي تعتبر البنية التحتية لإقامة تجارة إلكترونية، وكذا إلى وسائل الدفع الالكترونية، باعتبارها مرحلة مهمة من مراحل إتمام الصفقة أو العملية الإلكترونية.

1- وسائل إبرام العقود الالكترونية.

تعتمد التجارة الالكترونية على عدة وسائل حديثة، لعل من أبرزها الانترنت، لما تتميز به من خصائص عديدة، ويجوز أن تبرم عقود التجارة الالكترونية بأية وسيلة إلكترونية. ويمكننا أن نستعرض بعض وسائل إبرام عقود التجارة الالكترونية على النحو الآتي:

– **جهاز المينيتال:** هو جهاز قريب الشبه بجهاز الكمبيوتر، ولكنه صغير الحجم، ظهر في فرنسا في منتصف الثمانينيات، وهو عبارة عن وسيلة اتصال مرئية تنقل الكتابة إلى جهاز منيتال آخر، دون الصور، وهو بذلك وسيلة لإبرام عقود التجارة الالكترونية.[4]

---

[1] محمد الصيرفي، المرجع السابق، ص152.

[2] مصطفى كمال طه، وائل أنور بندق، الأوراق التجارية ووسائل الدفع الالكترونية الحديثة، دار الفكر الجامعي، الإسكندرية، مصر 2006. ص327.

[3] محمد الصيرفي، المرجع السابق، ص154.

[4] إيمان مأمون أحمد سليمان، إبرام العقد الالكتروني وإثباته، دار الجامعة الجديدة، الإسكندرية، مصر 2008، ص84.

– **جهاز التلكس**: هو جهاز لإرسال البيانات، عن طريق طباعتها وإرسالها مباشرة، وتتم العملية على شبكة خاصة مراقبة من مركز رئيس للاتصالات، وسيط ومحايد، يحدد هوية المتراسلين، ويكفل استعداد الجهاز المستقبل للاستقبال، ويؤرخ العملية، ويحتفظ بما يثبت وقوعها لمدة سنة مما يوفر الأمان، غير أن الرسالة المبعوثة عن طريق هذا الجهاز غير موقعة من طرف العميل، مما قد يؤدي إلى حدوث الغش، ولكن رقم التلكس يظهر على أعلى الرسالة وفي أسفلها. وقد أقر القضاء الفرنسي والبلجيكي والانجليزي بحجية التلكس في الإثبات.[1]

– **الفاكس**: هو عبارة عن جهاز نسخ بالهاتف، يتم عن طريقه نسخ الرسائل نسخا مطابقا للأصل، إلى جهاز فاكس آخر مرسل إليه. والملاحظ أن هناك فاصلا زمنيا للرد على المرسل. وقد توافرت عوامل الثقة في التعامل بالفاكس، خاصة في كل من أوربا والو. م. أ. [2]

– **التيليفون أو الهاتف**: يستخدم هذا الجهاز من أجل إبرام عقود التجارة الالكترونية، ويتميز بسرعة الاتصال وسهولة الاستخدام، ويتم التعاقد بواسطته فوريا ومباشرا.[3] ويستخدم أيضا الهاتف الخلوي أو النقال في إبرام العقود الالكترونية.

– **التيليفزيون**: يستخدم هذا الجهاز أيضا في إبرام عقود التجارة الالكترونية، ويكون ذلك حينما يقوم مقدم البرنامج بعرض السلعة المراد بيعها أو الخدمة، وتحديد أوصاف المبيع والسعر، وقيام المتفرج بالاتصال بالبرنامج لإبداء رغبته في شراء السلعة، أو الاستفادة من الخدمة، مع ترك بياناته، فتصله السلعة بمكان إقامته.[4] وتحقق التجارة عبر التليفزيون أرباحا معتبرة في الو.م.أ وفرنسا، هذه الأخيرة صدر بها سنة 1988 قانون لتنظيم مثل هذه البيوعات سمي قانون: "Télé-Achat".[5]

– **جهاز الكمبيوتر أو الحاسب الآلي**: يعتبر هذا الجهاز من أكثر الأجهزة استعمالا في مجال التجارة الالكترونية، خاصة عن طريق الانترنت. رغم أن الإبحار في الانترنت قد يتم بأجهزة إلكترونية عديدة كالهاتف المحمول مثلا، إلا أن الكمبيوتر لا يزال هو الجهاز الأكثر استعمالا. تتعدد وسائل التعاقد عبر شبكة الانترنت، فقد تتم عن طريق المراسلة من خلال البريد الالكتروني، وقد تتم عن

---

[1] المرجع نفسه، ص85.

[2] إيمان مأمون، المرجع السابق، ص86.

[3] المرجع نفسه، ص87.

[4] المرجع نفسه، ص87.

[5] المرجع نفسه، ص88.

طريق المحادثة أو المشاهدة، وقد تتم أيضا عن طريق شبكة المواقع "ويب"، وهذه الأخيرة تعتبر الأكثر انتشارا بالنسبة للتعاقد عبر الانترنت.[1]

كما تبرم عقود التجارة الالكترونية عن طريق الانترنت، فإنه يجوز أن تبرم أيضا عن طريق الأنترانت، أو الإكسترانات.

فالأنترانت شبكة خاصة تعتمد على الانترنت من أجل تكوين شبكات داخلية لمشروعات شركة أو مؤسسة دون غيرها، وتستخدم فيها الوسائل التأمينية المختلفة مثل وسائل التشفير والحوائط النارية.[2]

أما الإكسترانت فهي عبارة عن شبكة خاصة، ملك لمؤسسة معينة، تستخدم في إجراء عمليات الاتصال وتبادل المعلومات بين المؤسسة ومختلف المتعاملين معها، بصورة آمنة، وهي بذلك على خلاف الأنترانت الداخلية الخاصة بالمؤسسة، تتيح الاستخدام لأطراف من خارج المؤسسة وفروعها. وتستعمل هذه الشبكة أيضا الوسائل التأمينية المختلفة على غرار الأنترانت.[3]

2- وسائل الدفع الإلكترونية.

تعتمد التجارة الالكترونية بالإضافة إلى وسائل الدفع التقليدية، على وسائل جديدة للدفع تتناسب وطبيعتها الخاصة، وهي عبارة عن وسائل دفع إلكترونية، تمكن أصحابها من الوفاء بالتزاماتهم المالية عن بعد،[4] ومن أبرز هذه الوسائل ما يلي:

- **بطاقات الوفاء وبطاقات الائتمان:** هي وسيلة للوفاء، والائتمان، وهي أداة تسمح لحاملها اتخاذ الإجراءات اللازمة والمباشرة لخصم المبلغ الذي يحدده لمصلحة شخص آخر من حسابه لدى البنك الذي أصدر هذه البطاقة،[5] وتسمح هذه البطاقة لحاملها بتنفيذ مشترياته من السلع والخدمات

---

[1] المرجع نفسه، ص 89.

[2] إيمان مأمون، المرجع السابق، ص93.

[3] المرجع نفسه، ص94.

[4] عصام عبد الفتاح مطر، التجارة الالكترونية في التشريعات العربية والأجنبية، دار الجامعة الجديدة، الإسكندرية، مصر2009، ص77.

[5] محمد صبحي نجم، المسؤولية الجزائية عن الاستخدام غير المشروع لبطاقات الائتمان، بحث مقدم لمؤتمر الأعمال الالكترونية بين الشريعة والقانون، المجلد الثالث، ص1161.

الالكترونية من كبرى الشركات العالمية ومواقعها على شبكة الانترنت دونما حاجة لوفاء فوري،[1] ويطلق الكثير من الكتاب مسمى بطاقة ائتمان على كل أنواع البطاقات بدون توضيح معيار التمييز بين بطاقات الوفاء والائتمان، للتماثل الكبير بين نوعي البطاقات من حيث الشكل، والمادة المستخدمة، والوظيفة، ومعيار التمييز بين البطاقتين يكمن في المدة الممنوحة للحامل، والتي تمنحه ائتمانا يسمح بتنفيذ عمليات شراء، أو الحصول على خدمات بمقابل هذه العمليات فيما بعد على أقساط، لذلك يرى البعض أن بطاقة الائتمان ما هي إلا بطاقة وفاء مقيدة بخط اعتماد متجدد، عبارة عن حساب جار يفتح للعميل، يكون محددا بحد أقصى لكل حامل تبعا لائتمانه الشخصي، وهذا الحد المسموح به يتجدد تلقائيا، فإذا ما نقص بالشراء المنفذ بالبطاقة فإنه يتجدد بأي مبالغ يردها الحامل شهريا، والهدف هو تقسيط النفقات، والحصول على إمكانية التصرف في رصيد دائم لمواجهة ما يستجد من نفقات.[2]

وبطاقات الائتمان أو الوفاء أنواع كثيرة منها بطاقة ضمان الشيكات، بطاقة السحب الآلي، البطاقة الفضية، البطاقة الذهبية، البطاقة الماسية، وبطاقة الانترنت.[3]

– **البطاقة الذكية:** هي بطاقة بلاستيكية، ذات ميكروسوفت مدمج يحتوي على بعض المعلومات والبيانات التي يمكن استرجاعها في أي وقت. ويحبذ البعض إدراجها تحت بند البطاقات أو الأموال البلاستيكية، كونها ليست إلا جيلا جديدا من البطاقات.[4] ويفضل البعض الآخر إدراجها ضمن النقود الالكترونية، لأنه بالإمكان تخزين قيم النقود عليها، على عكس البطاقات العادية، التي تستخدم كأداة لسحب المبالغ من البنوك، ويرى جانب ثالث من الفقه، أنه بالنظر لأهميتها فإنها تعتبر وسيلة مستقلة للدفع الالكتروني.[5]

---

[1] محمد نور الدين سيد عبد المجيد، المسؤولية الجنائية عن الاستعمال غير المشروع لبطاقات الوفاء والائتمان، دراسة مقارنة، دار النهضة العربية، القاهرة، مصر 2008، ص11.

[2] محمد نور الدين سيد عبد المجيد، المرجع السابق، ص14.

[3] عصام عبد الفتاح مطر، المرجع السابق، ص84-85.

[4] المرجع نفسه، ص85.

[5] المرجع نفسه، ص86.

وتتميز هذه البطاقة بمواصفات أمان عالية يصعب معها قيام الغش المعلوماتي،[1] وتستخدم في الوم.أ في مجالات شتى.[2] ومن أشهر البطاقات الذكية البطاقة الذكية موندكس.

– **الشيكات الالكترونية:** بعض المؤسسات المالية تعمل على تكييف وسائل الدفع المعروفة لتتلاءم مع مقتضيات التجارة الالكترونية، لذا جرى تطوير استخدام الشيكات الورقية إلى نظام الشيكات الالكترونية.[3]

والشيك الالكتروني عبارة عن رسالة إلكترونية موثقة ومؤمنة يرسلها مصدر إلى حامل، يعتمده ويقدمه للبنك الذي يعمل عبر الانترنت، ليقوم البنك لتحويل قيمته إلى حساب حامل الشيك، ثم إلغاء الشيك وإعادته إلكترونيا إلى حامله، كي يكون دليلا على أنه قد تم صرف الشيك فعلا، ويتعين وجود وسيط يجري عملية المقاصة، غالبا ما يكون أحد البنوك.

تبدأ عملية استخدام الشيك الالكتروني، في التجارة الالكترونية، بقيام المشتري بفتح حساب جار لدى أحد البنوك، أين يتم تحديد التوقيع الالكتروني له، وتسجيله في قاعدة البيانات الخاصة بالبنك. ويجب أن يكون للبائع حساب بالبنك ذاته، وأن يتم تحديد التوقيع الالكتروني له، وتسجيله بقاعدة البيانات الخاصة بالبنك.

ويقوم المشتري بتحرير شيك إلكتروني للبائع مقابل السلعة أو الخدمة، ويوقعه بالتوقيع الالكتروني المشفر، ويرسله عبر البريد الالكتروني إلى البائع.[4]

يقوم البائع باستلام الشيك الالكتروني، والتوقيع عليه كمستفيد، ويرسله إلى البنك الذي يقوم بمراجعته والتأكد من بياناته ورصيده، ويقوم بإخطار كل من البائع والمشتري بإتمام إجراء المعاملة المالية.[5]

---

[1] المرجع نفسه، ص86.

[2] فهي تستخدم في النقل العمومي، وفي الوفاء عبر الانترنت، وكحافظة نقود إلكترونية، وكبديل لجواز السفر وتذكرة السفر، ينظر: المرجع نفسه، ص87.

[3] المرجع نفسه، ص88.

[4] عصام عبد الفتاح مطر، المرجع السابق، ص90.

[5] المرجع نفسه، ص91.

– **النقود الالكترونية**: النقود الرقمية أو الالكترونية، عبارة عن بطاقات إلكترونية، تحتوي على مخزون نقدي يصلح كوسيلة للدفع، وأداة للإبراء، ووسيطا للتبادل.[1]

وتختلف صور هذه النقود وفقا للوسيلة التي يتم من خلالها تخزين القيمة النقدية، وكذا وفقا لحجم القيمة النقدية المخزنة على البطاقة، ومن أمثلتها البطاقة سابقة الدفع، والنقود الشبكية، والبطاقات ذات القيمة النقدية البسيطة والبطاقات ذات القيمة النقدية المتوسطة.[2]

يتعين للحصول على النقد الالكتروني أن يفتح المستهلك حسابا في بنك، وعندما يريد المستهلك أن يسحب النقد الالكتروني للقيام بعملية شراء، فإنه يدخل إلى البنك من خلال الانترنت، مقدما دليل شخصيته التي عادة ما تكون شهادة رقمية، تصدرها سلطة اعتماد، يقوم البنك بعد التحقق من هوية المستهلك، بإصدار المبلغ من النقد الالكتروني الخاص به، ويخصم المبلغ نفسه من حسابه بالإضافة إلى عمولة البنك، ويمكن للمستهلك صرف نقوده الالكترونية في مواقع التجارة الالكترونية التي تقبل النقد الالكتروني كوسيلة للسداد.

يرسل إلى التاجر نقد إلكتروني مقابل السلع أو الخدمات، حينها يتأكد التاجر من سلامة النقد الالكتروني، وعندما تشحن السلع أو تقدم الخدمات فعلا إلى المستهلك، يقوم التاجر بتقديم النقد الإلكتروني إلى البنك المصدر للإيداع، وحينئذ فإن البنك يقيده دائنا في حساب التاجر بمبلغ الصفقة مخصوما منه مقابل الخدمة.[3]

من أكثر الشعوب استخداما للنقد الإلكتروني اليابانيون، وقد بدئ استخدامها أولا في القطارات السريعة، ثم عمم استعمالها،[4] وتقوم فلسفتها على عكس فلسفة بطاقات الائتمان، فهي موجهة للزبائن الذين يرغبون في دفع مشترياتهم مسبقا.[5]

---

[1] المرجع نفسه، ص91.

[2] المرجع نفسه، ص92- 93.

[3] عصام عبد الفتاح مطر، المرجع السابق، ص94.

[4] د. أمير فرج يوسف، بطاقات الائتمان والحماية الجنائية لها، دار المطبوعات الجامعية، الإسكندرية، مصر 2008.

[5] المرجع نفسه، ص54.

يرى العض أن النقود الإلكترونية تحل بعض المشاكل المتعلقة بالدفع الإلكتروني، وأبرزها مشكلة الخصوصية أي البيانات المتعلقة بالمستهلك والتي تطلبها المواقع عندما يريد المستهلك القيام بعملية شراء،[1] لكنها تثير مشكلة الصرف المزدوج، ولذا لجأت البنوك إلى طلب جزء من معلومات المستهلك الشخصية على كل عملة يقوم بصرفها، فإذا قام بالصرف المزدوج أمكن وضع هذه الأجزاء معا لمعرفة هوية الفاعل.[2]

ويثور التساؤل التالي: هل البطاقات تعتبر نوعا من النقود الالكترونية؟

النقود هي وسيلة للوفاء، غير محددة، عامة وفورية، وهي تحظى بالقبول والثقة في التداول وإتمام المعاملات، وتختلف البطاقات عن النقود من حيث كون الأخيرة قابلة للتداول بمجرد تسليمها، في حين أن البطاقات غير خاضعة للتداول، فهي لا تستخدم إلا من قبل حاملها فقط كونها اسمية تخص الشخص الصادرة باسمه، كما أن ملكية النقود مرتبطة بقاعدة الحيازة في المنقول سند الملكية، ولا تنطبق هذه القاعدة على البطاقات، كما أن استخدام النقود يقوم على علاقة ثنائية بين الدافع والمدفوع له، أما البطاقة فأطرافها ثلاثة، ومعاملاتها لا تنتهي بمجرد إطلاع التاجر عليها، بل لا بد من حصول التاجر على حقه نقدا من البنك، وعليه يصعب التسليم بالرأي القائل بأن بطاقات الوفاء بصفة خاصة تعد نوعا من النقود يطلق عليها النقود الإلكترونية، إذ أن الأخيرة تعرف بأنها: "قيمة نقدية مخزنة على وسيلة إلكترونية مدفوعة مقدما، وغير مرتبطة بأرصدة بنكية أو حساب بنكي، وتتمتع بقبول عام سواء مصدرها أو غيره"وهذا التعريف متلائم مع ما جاء به تعريف التوجيه الأوربي رقم 2000/46 الصادر في 2000/9/18 إذ عرف النقود الإلكترونية بأنها: "قيمة نقدية مخلوقة من المصدر مخزنة على وسيط إلكتروني، تمثل إيداعا ماليا، تكون مقبولة كوسيلة دفع من قبل الشركات المالية غير الشركة المصدرة".

من استعراض ما سبق يمكن القول أن البعض وقع في خلط بين القيمة النقدية التي تمثل رصيد البطاقة، وبين البطاقة ذاتها كوسيط إلكتروني يتم تحويله بهذه القيمة النقدية من الأرصدة البنكية، فالنقود الإلكترونية هي القيمة النقدية وليست البطاقات.[3]

---

[1] المرجع نفسه، ص55.

[2] المرجع نفسه، ص58.

[3] محمد نور الدين، المرجع السابق، ص40 وما بعدها.

– **المحفظة الالكترونية:** هي إحدى وسائل الوفاء التي تصلح لسداد المبالغ قليلة القيمة، وهي عبارة عن تطبيق إلكتروني يقوم على أساس ترتيب وتنظيم آلية جميع الحركات المالية، وتتكون هذه المحفظة من بطاقة بلاستيكية مثبت عليها من الخلف كمبيوتر صغير مزود بذاكرة إلكترونية تسمح بتخزين معلومات ووحدات إلكترونية تصلح للوفاء بالديون قليلة القيمة، عند التاجر أو على شبكة الانترنت. وتسمح الذاكرة أيضا بتخزين نقود إلكترونية في وحدات يتم استخدامها في سداد قيمة المعاملات التي يجريها العميل، دون أن ترتبط بحساب معين للعميل.[1] ومن تطبيقات هذه المحافظ، محفظتا النقود الفرنسية "Monéo" وحدها الأقصى الذي يجوز شحنها به 100 يورو، و"Modéus"، والمحفظة الانجليزية "Modex".[2]

المطلب الثاني: واقع وآفاق التجارة الالكترونية

يتم التطرق من خلال هذا المطلب إلى أهم التحديات التي تواجه التجارة الالكترونية، خاصة بدول العالم الثالث (الفرع الأول)، ثم محاولة رصد واقع وآفاق التجارة الالكترونية بالجزائر (الفرع الثاني).

الفرع الأول:عوائق و تحديات التجارة الإلكترونية

يعالج هذا الفرع من خلال التطرق في نقطة أولى إلى أهم التحديات التي تواجه التجارة الالكترونية بصفة عامة، وفي نقطة ثانية إلى التخلف التكنولوجي لدول العالم الثالث، وعدم قدرتها على مواكبة ركب التقنيات المتطورة، وهو ما يعرف بالفجوة الرقمية، وما يمكن أن يشكله هذا التخلف التكنولوجي من خطر على هذه الدول.

أولا: عوائق التجارة الالكترونية.

تواجه التجارة الالكترونية جملة من العوائق والعقبات تقف حجر عثرة أمام تطورها وانتشارها، ومن أبرزها:

[1] عصام عبد الفتاح مطر، المرجع السابق، ص98.

[2] المرجع نفسه، ص ص100- 101.

1- : العقبات النفسية والثقافية

لا يزال العامل النفسي يشكل تحديا للتجارة الالكترونية، فبعض المتعاملين لا يتقبلون إبرام الصفقات من خلال شبكة الانترنت، خاصة إذا كانت قيمتها معتبرة، أو يفضلون إبرام الصفقات إلكترونيا والسداد بأسلوب تقليدي، وذلك نتيجة نقص في الثقة بالمعاملات الالكترونية.[1] كما أن الثقافة الالكترونية لا تزال لم تأخذ مكانتها الطبيعية في كثير من البلدان، وهناك دول مستوى ونوعية التعليم فيها محدود، مما ينعكس سلبا على نشر الثقافة والاستخدام الالكتروني.[2]

2- العقبات التقنية

هنالك العديد من العقبات التقنية التي تواجه التجارة الالكترونية، خاصة بدول الجنوب، ومن أهمها ضعف تحويل قدرات التحويل وتصميم البرامج إلى طاقات إنتاجية مؤثرة لقطاعات تكنولوجيا الإعلام والاتصال، ضعف أنشطة البحوث والتطوير، وتواضع مستوى وأعداد الباحثين في مجال التجارة الالكترونية في الدول المتخلفة، وضعف البنية التحتية الالكترونية، بالإضافة إلى عدم تبني حكومات دول الجنوب استراتيجيات شاملة للتعامل مع تكنولوجيا الاتصالات.[3]

3- العقبات التجارية.

ومن أهمها، محدودية حجم التجارة الالكترونية نسبيا سواء بين الشركات التجارية نفسها، أو بينها وبين مورديها المحليين، وبينها وبين المستهلكين، وكذا قصور الأسواق المالية في الكثير من دول الجنوب عن دعم مشروعات التجارة الالكترونية، وعجز الاستراتيجيات الحكومية لدعم المشروعات التجارية الوطنية لمنافسة نظيراتها العالمية.[4]

4- العقبات التشريعية

إن أي مستجدات حديثة تطرأ على المجتمع لا بد أن يحتضنها تطور تشريعي، ينظمها ويحتويها. والتجارة الالكترونية تختلف عن التجارة التقليدية التي وجدت التشريعات المختلفة لتنظيمها

[1] مصطفى كمال طه ووائل أنور بندق، المرجع السابق، ص338.

[2] عصام عبد الفتاح مطر، المرجع السابق، ص122.

[3] عصام عبد الفتاح مطر، المرجع السابق، ص121.

[4] المرجع نفسه، ص122.

وحل مشاكلها، ويكمن الفرق في وسائل هذه التجارة المتقدمة، والتي تمنحها خصائص متميزة، ولكنها في الوقت نفسه تثير الكثير من التحديات القانونية على أكثر من صعيد، سواء أتعلق الأمر بمرحلة ما قبل إبرام العقد الالكتروني، أو مرحلة إبرام العقد، أو مرحلة تنفيذ العقد. ومن أبرز هذه التحديات تحدي خصوصية العلاقة بين المتعاقدين، وخصوصية المعلومات المتداولة بينهما، وتحدي حماية التجارة الالكترونية من الأنشطة الإجرامية، ناهيك عن مشكلة الاختصاص القضائي في نظر المنازعات التي قد تنشأ بين أطراف العلاقة التعاقدية الالكترونية، فأي قضاء يحكم النزاع؟ وأي قانون يطبق عند اختلاف جنسية المتعاقدين؟

كما أن هناك تحديات تواجه الملكية الفكرية، تتمثل في حماية عناصر الملكية الفكرية في بيئة التجارة الإلكترونية، وتحديدا حماية العلامات التجارية وأسماء النطاقات ورخص المنتجات المباعة والمخزنة داخل النظم التقنية وكجزء من المبيع، ومحتوى مواقع التجارة الإلكترونية، وحقوق النشر الإلكتروني، خاصة مع تزايد ظاهرة الاستيلاء على التصاميم التي يستخدمها موقع ما أو منتج.[1]

ثانيا: دول العالم الثالث والفجوة الرقمية

رغم أن مصطلح الفجوة الرقمية، أو الشرخ أو الهوة الرقمية، جديد، إلا أن مفهومه قديم قدم استعمال الإنسان لوسائل وتقنيات تسخير الطبيعة، غير أن سعة الفجوة أكبر في مجتمع المعلومات منها في المجتمعات السابقة.[2]

والحقيقة أنه ليس ثمة فجوة رقمية واحدة، بل فجوات، حيث تذكر المراجع المتخصصة ما لا يقل عن أربعة، وهي: فجوة في الوصول إلى استخدام تكنولوجيا المعلومات والاتصالات، وتقاس شكليا بمدى انتشار خطوط الهاتف، وأجهزة الكمبيوتر الموصولة بالانترنت وغيرها، وفجوة في القدرة على استخدام تكنولوجيا المعلومات، تقاس بمستوى المهارات وبوجود العديد من المكملات النشطة، وفجوة في الاستخدام الفعلي، تقاس من خلال الوقت المستغرق في الاتصالات السلكية واللاسلكية لأغراض مختلفة، بعدد مستخدمي الانترنت والوقت المستغرق في ذلك، بعدد مضيفي الانترنت، وبمستوى التجارة الالكترونية وغيرها، وفجوة في أثر الاستخدام، وتقاس بالعوائد المالية والاقتصادية.

---

[1] عصام عبد الفتاح مطر، المرجع السابق، ص125.

[2] فضيل دليو، الفجوات الرقمية في عصر العولمة، مخبر علم اجتماع الاتصال للبحث والترجمة، جامعة قسنطينة، الجزائر 2010، ص185.

ويرى بعض الباحثين أن أهم مؤشر هو مؤشر الاختلاف في القدرة على استغلال التكنولوجيا الجديدة.[1]

ويستعمل مصطلح الفجوة الرقمية لوصف أنماط عدم المساواة في الوصول إلى تكنولوجيا المعلومات والاتصالات بين الدول، فالتفاوت في التقدم التكنولوجي من دولة إلى أخرى سوف يقسم العالم إلى مجموعتين، دول مصدرة للتكنولوجيا، وأخرى مستوردة لها، مما ينعكس بدوره على التجارة الالكترونية التي تعتمد في المقام الأول على أجهزة إلكترونية، وبرامج ونظم معلوماتية، تتقدم فيها دول الشمال على دول الجنوب، ولذلك فإن دول العالم المتقدم هي الأوفر حظا في مجال التجارة الالكترونية حيث ستقوم بتسويق مختلف منتجاتها وخدماتها إلى الطرف الآخر الأقل تقدما وهو الدول السائرة في طريق النمو، والتي ستكتفي بتلقي السلع والخدمات وقليل من التكنولوجيا من دول العالم المتقدم.[2]

ومنذ السبعينيات من القرن الماضي انتقدت الكثير من دول الجنوب، والمنظمات الدولية وخاصة اليونسكو تدفق المعلومات في اتجاه واحد، ولكن المتغيرات السياسية والتكنولوجية المتسارعة على المسرح العالمي، أبقت سيطرة الدول المتقدمة، وخاصة تلك المهيمنة على مؤسسات الإنتاج والتوزيع، وذات البنية التحتية المتطورة.[3]

ويستخدم مصطلح الفجوة الرقمية لوصف أنماط عدم المساواة في الوصول إلى تكنولوجيا المعلومات والاتصالات في البلد الواحد، فهناك فجوات بين المناطق الحضرية وخاصة العواصم والمدن الكبرى، والمناطق الريفية، وكذا بين الأغنياء والفقراء، بل هناك فجوات بسبب مؤشرات السن والجنس، واللغة والعرق، والمستوى التعليمي والمهنة وسلامة الجسم...[4]

يؤكد خبراء الاقتصاد أن هناك اقتصادا جديدا، يقوم على السلع غير المادية، ويتعامل بالأفكار، وعناصرها من المعلومات، كبديل عن السلع المادية، والأجهزة والعملات النقدية المباشرة، لهذا يركز هذا الاقتصاد في صورته الالكترونية على الخدمات، وتظهر فيه أهمية المعلومات التي صارت

---

[1] المرجع نفسه، ص186.

[2] عبد الفتاح بيومي حجازي، التجارة الالكترونية وحمايتها القانونية، الكتاب الأول، ص ص71-72.

[3] فضيل دليو، المرجع السابق، ص188.

[4] المرجع نفسه، ص187.

ثروة العديد من الدول حيث بلغت 80% من دخلها القومي، لذلك فالتقدم التكنولوجي والتجارة الالكترونية معلومات ذات قيمة، متداولة عبر النظم المعلوماتية.[1]

لذلك لا مجال أمام الدول المستهلكة للتكنولوجيا، إلا أن تسعى جاهدة لتطوير نظمها المعلوماتية والتشريعية، ومحاولة الحصول على التكنولوجيا بإمكاناتها الذاتية، والدخول في اتفاقيات جادة مع الدول المتقدمة في هذا الخصوص، خاصة وأن الدول المتقدمة، ارتبطت مع بقية الدول باتفاقية دولية لحماية الملكية الفكرية "Trips" تجعل من الصعب نقل التكنولوجيا للدول الأخرى إلا من خلالها هي.[2]

وبخصوص الدول العربية فإن الدراسات تشير أن الكثير من الدول العربية (خاصة غير الخليجية) لا تزال غير موجودة على الخريطة الدولية للتجارة الالكترونية، التي تتم على الانترنت، و لا يتوقع إحراز تقدم كبير في السنوات القليلة المقبلة في استخدام وتطبيق التجارة الالكترونية لأسباب عديدة أهمها ضعف البنية التحتية في مجال الاتصالات والمعلوماتية، وتأخر الدول العربية في اتخاذ إجراءات خاصة لتهيئة البيئة القانونية والمصرفية لتعاملات وتطبيقات التجارة الالكترونية، فضلا عن تدني مستوى الدخل والتعليم.[3]

وبغية التصدي لهذه العوائق أو التقليل منها كانت هنالك العديد من الجهود العربية، والدراسات التي أكدت على ضرورة إطلاق الحريات والتعبير والتنظيم وضمانها بالحكم الصالح، النشر الكامل للتعليم ذي النوعية الرفيعة، توطين العلم وبناء قدرة البحث والتطوير التقني، التحول الحثيث نحو نمط إنتاج المعرفة، وتأسيس نموذج معرفي عربي يقوم على صحيح الدين، والنهوض باللغة العربية، واستحضار التراث، وإثراء التنوع الثقافي داخل الأمة مع الانفتاح على الثقافات الأخرى.[4]

---

[1] عبد الفتاح بيومي حجازي، المرجع السابق، ص74.

[2] عبد الفتاح بيومي حجازي، المرجع السابق، ص ص76-77.

[3] محمد سعيد أحمد إسماعيل، المرجع السابق، ص ص71-72.

[4] فضيل دليو، المرجع السابق، ص202.

الفرع الثاني: واقع وآفاق التجارة الالكترونية بالجزائر.

يتم التطرق في نقطة أولى إلى واقع التجارة الالكترونية في الجزائر، وفي نقطة ثانية إلى آفاق هذه التجارة والحلول الممكنة للتغلب على مختلف العقبات.

أولا : واقع التجارة الالكترونية في الجزائر.

الحديث عن التجارة الالكترونية في الجزائر يقود أولا للحديث عن سياسات الجزائر في مجال الإعلام والاتصال، والمعلوماتية، وثانيا للحديث عن الانترنت في الجزائر.

يمكن إجمالا القول بأن الجزائر عرفت ثلاث مراحل كبرى في سياستها الموجهة إلى مجال الإعلام والاتصال،[1] المرحلة الأولى هي مرحلة السبعينيات، وفيها بادرت الدولة إلى إنشاء المحافظة الوطنية للإعلام الآلي، ومركز التكوين والبحث في الإعلام الآلي، وتبوأت الجزائر مكانة مرموقة من بين البلدان السائرة في طريق النمو في هذا المجال، بإنشاء المؤسسات، والاهتمام بالتكوين، وتصميم نظم معلوماتية، وإنجاز برمجيات، بل وتركيب العتاد الخاص بالإعلام الآلي. وسمحت هذه السياسة من البدء في إدخال النظام المعلوماتي على تسيير المؤسسات والإدارات، وإنجاز شبكات التسيير المعلوماتية لكل من مركز الحساب الجاري، وسوناطراك، والخطوط الجوية الجزائرية، وتكوين مئات المهندسين والتقنيين في الإعلام الآلي. أما المرحلة الثانية فهي مرحلة الثمانينيات والتسعينيات، فيها تراجعت الجزائر عن مكانتها المرموقة، نتيجة الأوضاع السياسية والأمنية والاقتصادية الحرجة التي كانت تمر بها. وأنشئ سنة 1986 مركز الدراسات والبحوث في الإعلام العلمي والتقني "cerist" الذي عهد إليه تسيير نطاق dz. أما المرحلة الثالثة فتبدأ من مشارف الألفية الثالثة، حيث سعت الجزائر إلى محاولة تدارك ما فاتها من تقدم تكنولوجي، فعمدت إلى إنشاء بنية اتصالات ذات قدرة كبيرة من الألياف البصرية طولها 45000كم، وإنشاء تنظيم جديد للاتصالات السلكية واللاسلكية، وفتح المجال للقطاع الخاص، إنشاء مؤسسات خاصة تتكفل بتزويد خدمات الانترنت، وتوفير الخدمات في مجال الإعلام التقني والاقتصادي والثقافي، بيع رخص استغلال نظم جديدة للاتصالات السلكية واللاسلكية مثل

[1] الأزرق بن عبد الله، أحمد عمراني، نظام المعلوملتية قي القانون الجزائري واقع وآفاق، بحث مقدم إلى المؤتمر السادس لجمعية المكتبات والمعلومات السعودية، الرياض2010، ص6 وما بعدها.

GSM، وVOLP، ظهور مقاهي الانترنت وارتفاع عدد مستعمليها، وتعميم استعمال الهاتف النقال.

في سنة 1994 ارتبطت الجزائر بالانترنت عن طريق إيطاليا، بسرعة ارتباط ضعيفة جدا قدرت ب: 9.6ko/s في إطار مشروع تعاون مع منظمة اليونسكو الهدف منه إقامة شبكة الانترنت في إفريقيا عن طريق الجزائر.[1]

وفي سنة 1996 وصلت سرعة الخط إلى 64 كيلو في الثانية، يمر عن طريق باريس، وفي سنة 1998، تم ربط الجزائر بواشنطن عن طريق القمر الصناعي بقدرة 01 ميغابيت في الثانية، ومنذ تلك الفترة وتدفق الانترنت في الجزائر في تزايد. كما وصل عدد مقدمي خدمة الانترنت في الجزائر إلى 120 شركة نهاية سنة 2004.[2] غير أن الخدمة كانت مركزة بشكل أكبر في المدن الشمالية الكبرى، خاصة تلك القريبة من الجزائر العاصمة،[3] وتشير الدراسات أن نسبة من يستعملون الانترنت في الجزائر لا تزال ضئيلة، ولعل ذلك يعود إلى غياب الثقافة المعلوماتية بين أفراد المجتمع، وإلى ضعف القدرة المعيشية.[4]

وبخصوص البنية التحتية للانترنت بالجزائر فإنها تعتمد بالدرجة الأولى على الخطوط الهاتفية، سواء أكانت أليافا بصرية، أو خطوطا لا سلكية تعتمد على الأقمار الصناعية أو تقنية البث بموجات الراديو الحديثة، أو الذبذبات المعتمدة في خدمات الهاتف النقال، أو حتى الخطوط الهاتفية التقليدية المتمثلة في كابلات الهواتف المعروفة، لذلك يجوز الربط بين مدى انتشار الانترنت في الجزائر، بمدى انتشار الخدمات الهاتفية ونسبة المشتركين فيها.[5]

---

[1] محمد مولود غزيل، معوقات تطبيق التجارة الالكترونية في الجزائر وسبل معالجتها، رسالة لنيل درجة الدكتوراه في العلوم الاقتصادية، تخصص إقتصاد التنمية، جامعة أبي بكر بلقايد، تلمسان 2010، ص197.

[2] محمد مولود غزيل، المرجع السابق، ص198.

[3] المرجع نفسه. ص199.

[4] المرجع نفسه، ص199.

[5] المرجع نفسه، ص102.

بخصوص جودة خدمة الانترنت المقدمة في الجزائر، فإنه ينبغي الأخذ في الحسبان عدد من العوامل: سعة التدفق التي توفرها شركات الاتصال، مدى التمتع بالتدفق ذاته على مدار اليوم والأسبوع، الأعطال المصاحبة للخدمة، سعر الخدمة، حرية الاستعمال والحماية، وغيرها من العوامل.

ثانيا: آفاق التجارة الالكترونية في الجزائر.

تولي الجزائر مجهودات معتبرة لتطوير تكنولوجيا الإعلام والاتصال وتعميمها، سواء على الصعيد الداخلي أو الخارجي، فعلى الصعيد الداخلي تم وضع برنامج طموح هو "الاستراتيجية الإلكترونية للجزائر لعام 2013"، وعلى الصعيد الخارجي أطلقت مبادرات إقليمية من مثل مشروع إمداد الليف البصري بين كل من الجزائر والنيجر والجزائر ونيجيريا، يندرج ضمن مشروع الشراكة الجديدة لإنماء إفريقيا.[1]

يتمثل برنامج "الجزائر الالكترونية" في مشروع يتكون من ثلاثة عشر محورا رئيسا،[2] يركز المحور الأول على تعزيز استخدام تكنولوجيا المعلومات والاتصالات في الإدارات الحكومية، أما المحور الثاني فيعنى بتطوير استخدام تكنولوجيا المعلومات والاتصالات في المنشآت التجارية، ويهتم المحور الثالث بوضع آليات وتدابير تشجيعية تسمح للمواطنين بالنفاذ إلى تجهيزات وشبكات الإعلام والاتصال، أما المحور الرابع فيهدف إلى تحفيز وتطوير الاقتصاد الالكتروني، من محتوى وخدمات، ويرمي المحور الخامس إلى تعزيز البنية التحتية للاتصالات للوصول إلى سرعة عالية، ويركز المحور السادس على وضع خطة دقيقة لتطوير الكفاءات البشرية، ويحتوي المحور السابع على برامج لتعزيز البحث والتنمية والابتكار، أما المحور الثامن فيهتم بالإطار التشريعي، ويهتم المحور التاسع بوضع وتنفيذ خطة اتصالات بشأن مجتمع المعلومات في الجزائر، وإقامة شبكة من التجمعات التشاركية كامتداد لجهود الدولة، ويؤكد المحور العاشر على أهمية التعاون الدولي، من خلال المشاركة الفعالة في الحوارات والمبادرات الدولية، وإقامة شراكات استراتيجية، أما المحور الحادي عشر فيركز على آليات التقييم والمتابعة الإلكترونية، بينما يركز المحور الثاني عشر على التدابير التنظيمية، أما المحور الثالث عشر والأخير فيعنى بالموارد المالية.

---

[1] محمد مولود غزيل، المرجع السابق، ص230.

[2] المرجع نفسه، ص239-240.

ولكن، ورغم التطور الملحوظ الذي تعرفه التجارة الالكترونية في الجزائر، ورغم نجاح بعض المواقع الجزائرية التي أصبحت لها مداخيل مهمة بفضل التجارة الالكترونية عبر الانترنت، إلا أنها تبقى محدودة مقارنة بما يمكن أن تحققه في حالة توفر الشروط الكفيلة بتسهيل العملية للاستغلال الأمثل للموارد المتاحة.[1]

المبحث الثاني: جرائم ومجرمو المعلوماتية.

يتم تقسيم هذا المبحث إلى مطلبين، يتناول الأول الجرائم المعلوماتية، أما الثاني فيتعرض إلى مجرمي المعلوماتية.

المطلب الأول: جرائم المعلوماتية.

إن من أخطر الجرائم الحديثة ما يعرف بالجرائم المعلوماتية، أو جرائم الكمبيوتر والانترنت، التي بدأ خطرها يتعاظم شيئا فشيئا، تزامنا مع تطور التكنولوجيا، ونمو عصابات الجريمة المنظمة التي تتخذ من جرائم تبييض الأموال وتجارة المخدرات والأسلحة غير المشروعة، وتجارة الرقيق الأبيض، وأعمال السرقة والابتزاز، والاحتيال المعلوماتي، والجرائم الإلكترونية على تنوعها حرفة لها.[2]

لما كانت شبكة الانترنت أحد أهم وأكبر نتاج أنتجته تكنولوجيا الاتصالات والمعلومات، فقد أوجدت هذه الشبكة جوا جديدا وملائما لظهور ونمو صور إجرامية مستجدة تمس قطاعات شتى من بينها التجارة الإلكترونية.

وثار خلاف فقهي حول مسمى الجرائم الواقعة في نطاق شبكة الانترنت بصفة خاصة، وفي البيئة الرقمية عموما، من أهمها: الجرائم المستحدثة، جرائم نظم المعلومات، جرائم الانترنت، الجرائم الالكترونية، جرائم الكمبيوتر والانترنت، جرائم التقنية العالية، الجرائم المعلوماتية، الجرائم السيبيرية، جرائم الاختراقات...[3] إلا أن مصطلح الجرائم المعلوماتية ومصطلح الجرائم الإلكترونية هما الأكثر استخداما من قبل الفقهاء والباحثين، ويرى بعضهم أنهما يعبران عن جرائم الحاسب الآلي وجرائم الانترنت معا، إلا أن هناك من يرى أن جميع هذه المصطلحات المستعملة منتقدة في جانب أو

[1] المرجع نفسه، ص274.

[2] عبد الله عبد الكريم عبد الله، جرائم المعلوماتية والانترنت، منشورات الحلبي الحقوقية، بيروت، لبنان 2007، ص13.

[3] سامح أحمد بلتاجي موسى، رسالة مقدمة لنيل درجة الدكتوراه في الحقوق، كلية الحقوق، جامعة الإسكندرية، 2010، ص46.

من آخر، وأن أفضل تعبير للدلالة عن هذه الجرائم هو: "جرائم تقنية المعلومات"،[1] وهو المصطلح المستخدم من قبل وزراء الداخلية والعدل العرب، الموقعين على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، بالقاهرة في 2010/12/21، أما المشرع الجزائري فاستخدم في القانون 09-04 سالف الذكر مصطلح "الجرائم المتصلة بتكنولوجيا الإعلام والاتصال".

والمعلوماتية تعني "علم المعالجة الآلية للبيانات"، أو "استخدام التقنيات التكنولوجية في عملية معالجة البيانات (المعطيات) آليا بهدف الحصول على معلومات"، والمصطلح الفرنسي (informatique) يعني علم المعلومات، وهو اختصار لكلمة (information) وتعني المعلومة، وكلمة (automatique) وتعني آلي، والأمر ذاته بالنسبة للغة الانجليزية، وقد استخدم مصطلح "المعلوماتية" لأول مرة من قبل بعض الباحثين السوفييت كمرادف لمصطلح "علم المعلومات"، وتلقفه العالم ليستخدم في الو م أ، وبريطانيا، وبعض دول أوربا الشرقية، بمعنى التجهيز الآلي للمعطيات أو الأنشطة المتصلة بتصميم أجهزة الحاسب الآلي وإنتاجها واستخدامها، غير أن بعض الفرنسيين ينسبون المصطلح إلى الفرنسي "فيليب درافوس".[2]

الفرع الأول: مفهوم وخصائص جرائم المعلوماتية .

يتم التطرق أولا إلى مفهوم الجرائم المعلوماتية، ثم إلى أهم الخصائص المميزة لها.

أولا: مفهوم جرائم المعلوماتية.

توجد العديد من التعريفات المتعلقة بالظاهرة الإجرامية الناشئة في بيئة شبكة الانترنت، والبيئة الرقمية عموما، تتفق أحيانا وتتباين أخرى وفق الزاوية أو المنظور الذي نظر منه الباحث أو الفقيه للمسألة، وأغلب تلك التعريفات اعتمدت إما على المعيار القانوني، أو المعيار الشخصي، أو مزجت بين هذين المعيارين.

وفقا للمعيار القانوني فإن تعريف الظاهرة الإجرامية الواقعة في بيئة الانترنت يقوم إما على موضوع الجريمة وأنماط السلوك الإجرامي، أو على الوسيلة المستخدمة في ارتكاب الجريمة، فمن

---

[1] د. سرحان حسن المعيني، التحقيق في جرائم تقنية المعلومات، الفكر الشرطي، المجلد 20، العدد4، رقم 79، الشارقة، الإمارات العربية المتحدة 2011، ص23 وما بعدها.

[2] د. محمد حسن عبد الله علي، حماية برامج الحاسب بقانون براءة الاختراع في الولايات المتحدة الأمريكية، مجلة الشريعة والقانون، الإمارات العربية المتحدة، العدد 47، يوليو 2011، هامش ص120.

التعريفات المعتمدة على الموضوع تلك التي عرفت جرائم الانترنت بأنها: "جرائم تطال المعرفة، الاستخدام، الثقة، الأمن، الربح، المال، السمعة والاعتبار، ومع هذا كله فهي لا تطال حقيقة غير المعلومات"، ومن التعريفات المعتمدة على الوسيلة تلك التي عرفت الجرائم المعلوماتية بأنها: "جريمة يستخدم فيها الكمبيوتر كوسيلة أو أداة لارتكابها، أو يمثل إغراء بذلك، أو جريمة يكون الكمبيوتر ذاته ضحيتها"، أو:"هي كل فعل أو امتناع من شأنه الاعتداء على الأموال المادية أو المعنوية، يكون ناتجا بطريقة مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية".[1]

وقد وجهت انتقادات كثيرة للتعريفات القائمة على أساس الوسيلة، على اعتبار أنه يجب لتعريف الجريمة الرجوع إلى العمل الأساسي لها، وليس فقط إلى الوسائل المستخدمة لتحقيقه.[2]

أما التعريفات المعتمدة على المعيار الشخصي فتعني أن يتوافر في الجاني صفات معينة منها علمه ودرايته بالتقنية، ومن التعريفات وفق هذا المعيار: "الجريمة المعلوماتية هي أي جريمة يكون متطلبا لاقترافها أن تتوافر لدى فاعلها معرفة بتقنية الكمبيوتر"، أو هي: "واقعة تتضمن تقنية الكمبيوتر ومجني عليه يتكبد أو يمكن أن يتكبد خسارة، وفاعل يحصل عن عمد أو يمكنه أن يحصل على مكسب".

توجد تعريفات حاولت الجمع بين المعيارين القانوني والشخصي، منها تلك التي عرفت الجريمة المعلوماتية بأنها: "تلك الجرائم التي لا تعرف الحدود الجغرافية، والتي يتم ارتكابها بأداة معينة (الكمبيوتر) عن طريق شبكة الانترنت، بواسطة شخص على دراية فائقة بهما".

عبر خبراء المنظمة الأوربية للتعاون الاقتصادي عن الجريمة المعلوماتية بأنها: " كل سلوك غير مشروع أو مناف للأخلاق أو غير مسموح به، يرتبط بالمعالجة الآلية للمعطيات أو بنقلها".[3]

كما جاء في منظمة الأمم المتحدة العاشر لمنع الجريمة ومعاقبة المجرمين المنعقد في فينا تعريفها: "يقصد بالجريمة المعلوماتية أية جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية،

---

[1] عادل عبد الجواد محمد، إجرام الانترنت، مجلة الأمن والحياة، العدد 221، السنة 20، ديسمبر 2000/ يناير 2001، ص70.

[2] سامح أحمد بلتاجي، المرجع السابق، ص53.

[3] عبد الله عبد الكريم عبد الله، المرجع السابق، ص16.

أو داخل نظام حاسوب، وتشمل تلك الجريمة من الناحية المبدئية جميع الجرائم التي يمكن ارتكابها في بيئة إلكترونية".[1]

ومن الوارد جدا ألا يكون الهدف من وراء ارتكاب هذه الجرائم الحصولُ على منافع مادية، بقدر ما يكون بهدف التخريب أو الإضرار بالغير، أو إثبات الذات.

ولعل هذه الجرائم بدأت بالتزايد التدريجي مع سقوط المعسكر الشرقي وهيمنة الفكر الاقتصادي الغربي على اقتصاديات الدول، وما نتج عنه من انفتاح عالمي، وارتباط الأسواق العالمية بعضها ببعض، فأصبحت الأنشطة التجارية الممنوعة تتم عبر الحاسب الآلي وآلياته، وشبكة الانترنت، فأصبحت الجرائم تتم وتنظم بشكل إلكتروني.[2]

وتزيد خطورة هذه الجرائم عندما ينشأ تعاون غير مشروع لمجموعة من الخبراء، حيث تتلاقى أيدي خبراء المال والبنوك مع جهود الاقتصاديين والمجرمين وبعض القانونيين لتتجاوز العمليات الحدود الجغرافية لتضيفي سمة العالمية على الجريمة وصفة العولمة على تبعاتها ولجعلها جريمة منظمة بكل ما للكلمة من معنى في أغلب الأحيان.

من هنا بدأ الانشغال بإعداد استراتيجيات وطنية ودولية لمكافحة هذه الأنشطة، ورغم وسائلها المتعددة، إلا أن أشهرها يدور حول سرقة المعلومات والنفاذ بشكل غير قانوني إلى بعض المواقع الالكترونية عن طريق اختراقها والتلاعب بالحسابات المصرفية وأنشطة تبييض الأموال على الانترنت.

ثانيا: خصائص جرائم المعلوماتية.

من أهم خصائص الجرائم المعلوماتية أنها تستخدم الكمبيوتر كأداة لارتكاب الجريمة، إلا أن أي جهاز آخر يمكّن من الولوج إلى الانترنت أو إلى أي شبكة إلكترونية أخرى، يصلح كأداة لارتكاب الجريمة كالهواتف النقالة مثلا.

---

[1] محمد أمين أحمد الشوابكة، جرائم الحاسوب والانترنت، مكتبة دار الثقافة للنشر والتوزيع، عمان، الأردن 2004، ص10.

[2] المرجع نفسه، ص16.

ومن خصائص هذه الجرائم أيضا أنها غالبا ما تقع عبر شبكة الانترنت أو ضدها، بمعنى قد تكون شبكة الانترنت وسيلة لارتكاب جرائم معينة كالجرائم الواقعة على التجارة الالكترونية، أو تكون هي ذاتها هدفا للجرائم المعلوماتية، كالجرائم الواقعة على مواقع التجارة الالكترونية، غير أنه يمكن لأي شبكات أخرى أن تكون عرضة لهذه الجرائم.

ومن خصائص هذه الجرائم أيضا أن مرتكبيها يتمتعون بخبرة عالية في مجال الكمبيوتر والانترنت، كما يتمتعون بالذكاء الحاد، والرغبة في التحدي وإثبات الذات.

إذن، تتميز الجريمة المعلوماتية بطبيعة خاصة تجعلها متفردة عن غيرها من الجرائم التقليدية، وذلك نتيجة ارتباطها بالحاسب الآلي مع ما يتمتع به من تقنية عالية، وقد أضفت هذه الحقيقة على هذا النوع من الجرائم عددا من السمات والحقائق والتي انعكست بدورها على مرتكب هذه الجريمة، الذي أصبح يعرف بالمجرم المعلوماتي، لتميزه أيضا عن المجرم التقليدي، وقد كان لظهور شبكات المعلومات وتطورها، إلى الصورة التي أصبحت عليها الآن، أثره في إعطاء شكل جديد للجريمة المعلوماتية. ولعل أهم ما أضفته شبكات المعلومات على الجريمة المعلوماتية هو الطبيعة العالمية أو عبر الوطنية لهذه الجرائم.

تتميز الجريمة المعلوماتية بقلة عدد الحالات التي تم اكتشافها بالفعل إذا ما قورن ذلك في ضوء ما يتم اكتشافه من الجرائم التقليدية، ودليل ذلك ما تشير إليه الإحصاءات المختلفة، حيث تشير أنه لا يكتشف من هذه الجرائم إلا 01% فقط، أما نسبة الجرائم المعلوماتية المبلغ عنها فلا تتعدى 10%، ناهيك أن القضايا المطروحة أمام القضاء لم تكن أدلتها كافية إلا في حدود 20 % من القضايا،[1] ويرى البعض أنه من بين الأسباب وراء صعوبة اكتشاف هذه الجرائم تميزها بأنه لا يشوب ارتكابها أي عمل من أعمال العنف، كما أنها لا تترك آثارا وإنما يتمثل مظهرها في تغيير أو محو الأرقام والبيانات الموجودة بأنظمة الحاسبات الآلية، ولا تترك أثرا خارجيا مرئيا أو ملموسا، إلا أن جانبا من الفقه لا يستسيغ هذا الرأي المتقدم على إطلاقه، فمن ناحية لا يقتصر أثر جرائم المعلوماتية على تغيير أو محو الأرقام والبيانات من الملفات المخزنة في ذاكرات الحاسبات الآلية بل إنه حتى في هذه الحالات فمجرد تغيير أو محو هذه البيانات يعد أثرا على ارتكاب الفعل؛ فصعوبة اكتشافها

[1] عيشة خلدون، الطبيعة الخاصة للجريمة الإلكترونية وصورها، مجلة دراسات وأبحاث، العدد 09، جامعة الجلفة، الجزائر 2012، ص116.

وإثباتها يرجع إلى عدة أسباب من بينها وسيلة تنفيذها والتي تتسم في أغلب الحالات بالطابع التقني الذي يضفى عليها الكثير من التعقيد،[1] ناهيك عن الإحجام عن الإبلاغ عنها في حالة اكتشافها لخشية المجني عليه الذي عادة ما يكون مصرفا، أو مؤسسة مالية أو شركة أو مشروعا صناعيا مهما، من الإضرار بمركزه المالي، وللحفاظ على شعور المساهمين بالأمان والثقة، ومنعا لتكرارها عن طريق التقليد،[2] كما أن المجني عليهم قد لا يكتشفون تعرضهم لهذه الجرائم إلا بعد فوات مدة زمنية طويلة، فضلا عن إمكانية تدمير المعلومات التي يمكن أن تستخدم كدليل إثبات في مدة زمنية وجيزة قد لا تتعدى الثانية الواحدة.

من أهم الخصائص التي تميز الجريمة المعلوماتية، كونها عابرة للحدود، ومن ثم اكتسابها طبيعة عالمية، فبعد ظهور شبكة الانترنت لم تعد تشكل الحدود عائقا أمام نقل المعلومات عبر مختلف الدول، مما يجعل أماكن مختلفة من أنحاء شتى في دول العالم عرضة للجريمة المعلوماتية الواحدة في الوقت نفسه، كما أن السرعة الفائقة التي يتم من خلالها تنفيذ الجريمة المعلوماتية، وحجم المعلومات والأموال المستهدفة، والمسافات المترامية التي قد تفصل الجاني عن الضحية، كلها عوامل تميز الجريمة المعلوماتية عن الجريمة التقليدية بشكل واضح وكبير.[3]

وتظهر هذه المشكلة بصفة خاصة في مجال البنوك، حيث نتج عن التوسع الكبير في إجراء المعاملات البنكية عبر شبكات المعلومات الدولية إلى إعطاء بعد عالمي لجرائم الاحتيال المعلوماتي بصفة خاصة؛ فربط وسائل الاتصالات بالحاسبات الآلية ضاعف من المعاملات المالية الدولية التي تتم بوسائل إلكترونية وبصفة خاصة من خلال التحويل الإلكتروني للأموال، والتبادل الإلكتروني للمعلومات. ولا يقتصر الأمر على المعاملات المالية فقط، بل إن الطبيعة العالمية للجريمة المعلوماتية تظهر في أنماط أخرى من السلوك، فقد يوجد الجاني في بلد و يستطيع الدخول إلى الذاكرة المركزية لحاسب آلي موجود في بلد آخر، ويحيق الضرر تبعا لذلك بشخص آخر موجود في بلد ثالث، والأمر

[1] د. نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الاقتصادية، دراسة مقارنة، منشورات الحلبي الحقوقية، بيروت، لبنان 2005، ص49.

[2] عيشة خلدون، المرجع السابق، ص116.

[3] د. نائلة عادل محمد فريد قورة، المرجع السابق، ص52.

ذاته يتعلق بالإتلاف المعلوماتي، فإعداد أحد البرامج الخبيثة يمكن أن يحدث في دولة ما، ثم يتم نسخ هذا البرنامج آلاف المرات ويرسل إلى دول متفرقة من العالم.[1]

الفرع الثاني: أنواع الجرائم المعلوماتية وأضرارها.

يتم التطرق أولا إلى أنواع الجرائم المعلوماتية، حسب التقسيمات الفقهية، وثانيا إلى أضرار هذه الجرائم.

أولا: أنواع الجرائم المعلوماتية.

عموما، يكاد يجمع الفقه على أن الجرائم المعلوماتية على تنوعها واختلافها ، يجوز ردها إلى نوعين رئيسيين هما: الجرائم الواقعة على الحاسب الآلي أو النظام المعلوماتي ذاته، والجرائم الواقعة باستخدام النظام المعلوماتي.

---

[1] من القضايا التي لفتت الأنظار إلى البعد العالمي لجرائم الحاسب الآلي، قضية نقص المناعة المكتسبة "السيدا"، ففي سنة 1989 قام شخص بتوزيع عدد كبير من النسخ الخاصة ببرنامج يهدف في ظاهره إلى إعطاء بعض النتائج الخاصة المتعلقة بمرض نقص المناعة المكتسبة، بينما ظاهره من قبله المشاكل، إذ يحوي فيروس (حصان طروادة)، يترتب على مجرد تشغيله تعطل جهاز الحاسب الآلي عن العمل، ثم تظهر بعد ذلك عبارة على الشاشة يقوم الجانح من خلالها بطلب مبلغ من المال، يرسل على عنوان معين ببنما، نظير حصول المجني عليه على "مضاد للفيروس"، وقد تم القبض على المتهم في 1990/02/03، بالو م أ، وتقدمت بريطانيا بطلب تسليمه لها لمحاكمته أمام قضائها، لأن إرسال البرنامج كان من على أرضها، وهذا ما تم فعلا، ووجهت للمتهم إحدى عشرة تهمة ابتزاز، وقعت معظمها في دول مختلفة، إلا أن إجراءات محاكمة المتهم لم تستمر بسبب حالته العقلية. وأيا ما كان الأمر فإن لهذه القضية أهميتها من ناحيتين،الأولى: أنها المرة الأولى التي يتم فيها تسليم متهم في جريمة معلوماتية، والثانية: أنها المرة الأولى أيضا التي يقدم فيها شخص للمحاكمة بتهمة إعداد برنامج خبيث (فيروس). ولقد أثارت الطبيعة العالمية لجرائم الحاسبات الآلية تساؤلا مهما يتعلق بتحديد الدولة التي يختص قضاؤها بملاحقة الجريمة، فهل هي الدولة التي وقع بها النشاط الإجرامي أم تلك التي توجد بها المعلومات محل الجريمة أم تلك التي تضررت مصالحها نتيجة لهذا التلاعب. كما أثارت هذه الطبيعة أيضا الشكوك حول مدى فاعلية القوانين القائمة في التعامل مع الجريمة المعلوماتية، وبصفة خاصة فيما يتعلق بجمع وقبول الأدلة، حيث تتباين مواقف الدول المختلفة فيما يتعلق بقبول الأدلة المستخلصة من أنظمة الحاسبات الآلية. ومن القضايا التي لفتت النظر إلى هذه المشكلات، قضية "RV. Thompson "، وتتلخص وقائعها في قيام مبرمج إنجليزي يعمل بأحد بنوك الكويت بالتلاعب في نظام الحاسب الآلي الخاص بالبنك، بقيامه بإجراء خصومات من أرصدة العملاء، وإيداعها في حسابه الخاص. وبعد عودة الفاعل إلى انجلترا كتب إلى البنك بالكويت طالبا منه أن يقوم بتحويل الحساب الخاص به إلى حسابات بنكية عديدة بانجلترا، وهو ما قام به البنك فعلا. قدم المتهم إلى المحاكمة بتهمة الحصول على أموال الغير بطرق الاحتيال حسب نص م15 من القانون الانجليزي لسنة 1968 الخاص بالسرقة، وحكم عليه بعقوبة السجن، بيد أن المتهم طعن في الحكم بحجة عدم اختصاص القضاء الانجليزي باعتبار أن كلا من السحب والإيداع قد تما خارج بريطانيا (بالكويت)، ولكن محكمة الاستئناف رفضت الطعن المقدم، وردت بأن النشاط الإجرامي للمتهم لم يكتمل إلا بعد الطلب الذي تقدم به إلى مدير بنك الكويت، وكان هذا الطلب من الأراضي البريطانية، وما نتج عنه من حصوله على الأموال محل النشاط الإجرامي بواسطة البنوك الإنجليزية. يراجع: د. نائلة عادل محمد فريد قورة، المرجع السابق، ص52، وما بعدها.

1- الجرائم المعلوماتية الواقعة على النظام المعلوماتي.

بخصوص الجرائم الواقعة على النظام المعلوماتي أو الحاسب الآلي، فإنها لا تعدو أن تكون في أحد جانبيها، جرائم عادية أو تقليدية، تقع على المكونات المادية للحاسب الآلي، وفي هذه الحالة يمكن أن تكون هذه المكونات محلا للسرقة أو محلا للإتلاف العمدي، ويتحقق ذلك عن طريق إتلاف المكونات بالضرب بآلات حادة أو ثقيلة أو إشعال الحرائق أو تفجيرها بشحنات ناسفة أو استخدام قنبلة غاز أو مواد ملتهبة، أو العبث بمفاتيح التشغيل أو محو بطاقات التعريف بما فيها من معلومات مخزنة، أ و كشط الشريط أو مسحه، أو مسح البرنامج وإخفاء البطاقات، أو إفساد أسطوانات التشغيل ماديا، أو مغناطيسيا بتعريضها إلى أي مجال مغناطيسي متلف، ويترتب على هذا الإتلاف خسائر كبيرة، ومن أمثلة ذلك، ما حدث من تنظيم الألوية الحمراء بإيطاليا، حيث قامت مجموعة من المتخصصين لديهم في التكنولوجيا بتدمير مركز المعالجة الآلية لأحد الشركات بالديناميت مما نتج عنه خسائر بلغت قيمتها ما يربو عن المليون دولار أمريكي، كما خسرت شركة إيطالية أربعة أنظمة خاصة بها، بلغت قيمتها الإجمالية نحو أربعة ملايين دولار.[1]

وفي فرنسا حدثت أيضا حالات إتلاف لمعدات مؤسسة كبيرة متخصصة في بيع الأنظمة وتوثيق المعلومات الحسابية.[2]

هناك رأي فقهي في فرنسا يرى بأن كثيرا من الجرائم الواقعة على المكونات المادية للنظام المعلوماتي عبارة عن جريمة "سرقة وقت الآلة"، والتي تتم في الغالب من قبل العاملين بالنظام المعلوماتي عندما يقومون باستخدام النظام المعلوماتي لمصلحتهم الخاصة، وهنا لا تكون واقعة السرقة منصبة على أشياء مادية بمعنى الكلمة، وإنما على وقت الجهاز أو الآلة الذي يجوز تقويمه ماليا.[3]

ويمكن أن تكون المكونات المنطقية للحاسب الآلي هي محل الاعتداء، وهنا مكمن الخطورة، ويجوز القول أن هذه الجرائم تشمل الجرائم الواقعة على البرامج التطبيقية، وتقدر نسبتها بحوالي 15% من مجموع حالات الجرائم المعلوماتية، والغالب بالنسبة لهذا النوع من الجرائم قيام المجرم

[1] أحمد خليفة الملط، الجرائم المعلوماتية، دراسة مقارنة، ط2، دار الفكر الجامعي، الإسكندرية، مصر 2006، ص170.

[2] المرجع نفسه، ص171.

[3] المرجع نفسه، ص171.

المعلوماتي بتعديل البرنامج والتلاعب فيه بغية تحقيق أكبر نفع مالي ممكن أو لأسباب مختلفة؛[1] كما تشمل هذه الجرائم تلك الواقعة على برامج التشغيل المسؤولة عن عمل النظام المعلوماتي، وتتحقق بتزويد البرنامج بمجموعة تعليمات إضافية يسهل الوصول إليها بواسطة شفرة، تسمح بالحصول على كل معطيات النظام المعلوماتي، وتأخذ البرامج الواقعة على برامج التشغيل إحدى صورتين: المصيدة، وتصميم برنامج وهمي، من قبل المبرمجين من خلال برنامج تشغيل النظام المعلوماتي؛[2] كما تشمل هذه الجرائم الاعتداءات على المعلومات المدرجة بالحاسب الآلي، وتشمل التلاعب في المعلومات مباشرة، أو بطريق غير مباشر (عن بعد)، أو إتلاف المعلومات.[3]

2- الجرائم المعلوماتية الواقعة باستخدام النظام المعلوماتي.

يستخدم مجرمو المعلوماتية النظام المعلوماتي لارتكاب العديد من الجرائم، ومحلها الأموال والأشخاص، وإفشاء الأسرار العسكرية والسياسية والاقتصادية، مما ينتج عنه أضرار بالغة الخطورة على الدولة ككل، وعلى مصالح الأفراد، سواء بصفتهم أشخاصا طبيعيين، أو أصحاب مشروعات تجارية خاصة.

ومع النمو السريع لاستخدام شبكة الانترنت كوسيط تجاري تزايد انتشار الجريمة على هذه الشبكة، وتنوعت أشكالها بصورة مطردة، بداية من سرقة بيانات الحسابات المصرفية وبطاقات الائتمان من قبل محترفي اختراق الشبكات مرورا ببيع صور الأطفال على المواقع الإباحية وحتى قيام عصابات تبييض الأموال بإخفاء الأموال المتأتية من مصادر غير مشروعة، عبر عمليات معقدة من الحسابات المصرفية على شبكة الانترنت.[4]

وأهم صور الجرائم المعلوماتية ما يلي:[5]

- صناعة ونشر الفيروسات والاختراقات وتعطيل الأجهزة.

---

[1] من ذلك قيام موظف مفصول عن عمله ببرمجة النظام المعلوماتي للمؤسسة التي كان يعمل بها، بحيث يؤدي خلال ستة أشهر إلى اختفاء البيانات المتعلقة بديون المشروع كلها، مما أدى إلى إفلاس المشروع. الملط، المرجع السابق، ص172.

[2] عيشة خلدون، المرجع السابق، ص124.

[3] الملط، المرجع السابق، ص178 وما بعدها.

[4] عبد الله عبد الكريم عبد الله، المرجع السابق، ص24.

[5] المرجع نفسه، ص ص 25-31.

- انتحال الشخصية.
- الذم والتحقير والسب والشتم والإهانات عبر الانترنت.
- النصب والاحتيال في المعلوماتية.
- المواقع الإلكترونية التي تخفي نشاطها الأصيل وهو تبييض الأموال، كنوادي الانترنت المستخدمة في القمار.
- شراء المواقع الإلكترونية أو المنتديات على الشبكة العالمية، والتي تكون خاسرة أو متعسرة، والتي تكون معروضة للبيع، والهدف تمويلُها ثم تعويمها.
- جرائم انتهاك البيانات الشخصية الإلكترونية.
- جرائم الاعتداء على الأموال الإلكترونية.
- جرائم تزوير التوقيع الإلكتروني.
- جرائم استغلال المستهلك الإلكتروني.
- التحريض العمدي للقتل والعنف عبر الانترنت.
- الترويج للدعارة والفسق والانحلال الخلقي عبر الانترنت.
- التحرش والمضايقة عبر برامج المحادثات.
- أنشطة الاعتداء على الخصوصية.
- أنشطة الاعتداء على الخصوصية.
- جرائم المقامرة والجرائم المخلة بالآداب العامة والأخلاق.
- جرائم الاحتيال المعلوماتي.
- استخدام أسماء النطاق والعلامات التجارية دون ترخيص.
- استخدام الوسائل الإلكترونية للحصول على البطاقات المالية واستخدامها بشكل غير مشروع.
- جرائم تعطيل الأعمال الحكومية، كما في حالة تدمير المواقع الإلكترونية الخاصة باستخدام معاملات المواطنين المقدمة لإدارة معينة.
- الإرهاب الإلكتروني.

قسمت التشريعات المقارنة الجرائم المعلوماتية إلى عدة أقسام، ففي سنة 2001 وضعت الاتفاقية الأوروبية تقسيما لهذه الجرائم، أخرجت منه طائفة جرائم الخصوصية لوجود اتفاقية أوروبية

مستقلة تعالج حماية البيانات الاسمية من مخاطر المعالجة الآلية للمعطيات، وهي اتفاقية عام 1981، ولقد قسمت الاتفاقية الأوروبية لعام 2001، هذه الجرائم إلى أربع طوائف رئيسة؛ الطائفة الأولى تستهدف عناصر سرية وسلامة المعطيات والنظم، وتضم: الدخول غير القانوني أو غير المرخص له، الاعتراض غير القانوني، تدمير المعطيات، اعتراض النظم، وإساءة استخدام الأجهزة، أما الطائفة الثانية فتتعلق بالجرائم المرتبطة بالكمبيوتر وتضم: التزوير المرتبط بالكمبيوتر، والاحتيال المرتبط بالكمبيوتر، أما الطائفة الثالثة من الجرائم المعلوماتية فتتعلق بالجرائم المتعلقة بالمحتوى المعلوماتي وتضم طائفة واحدة وهي الجرائم المتعلقة بالأفعال الإباحية والمنافية للأخلاق، أما الطائفة الرابعة والأخيرة فتتعلق بالجرائم المتعلقة بالإخلال بحق المؤلف والحقوق المجاورة (قرصنة البرمجيات).[1]

أما مشروع القانون النموذجي الأمريكي فقد قسم هذه الجرائم تبعا لمساسها بالأشخاص أو بالأموال، فالجرائم التي تستهدف الأشخاص تضم طائفتين رئيستين هما: طائفة الجرائم الجنسية من مثل إغواء القصر لارتكاب أفعال جنسية غير مشروعة، وهذه الطائفة من الجرائم صورتها هي استغلال الانترنت والكمبيوتر لترويج الدعارة وإثارة الفحشاء واستغلال القصر في أنشطة جنسية غير مشروعة، وطائفة الجرائم غير الجنسية التي تستهدف الأشخاص كالقتل بالكمبيوتر، والتحريض على الانتحار، والاطلاع على البيانات الشخصية للغير، والانتهاك الشخصي لحرمة الكمبيوتر، والتجسس على البريد الالكتروني، والتشهير وتشويه السمعة...[2]

ثانيا: أضرار الجرائم المعلوماتية.

للجرائم المعلوماتية أضرار كثيرة ومخاطر عديدة، تستهدف بصفة مباشرة، الأمن والاستقرار السياسي والاقتصادي والاجتماعي، سواء على المستوى الوطني أو على المستوى الدولي؛ فالجرائم المعلوماتية بحكم طبيعتها تشكل انتهاكا لحدود وسيادة الدول، وتحديا صريحا أو ضمنيا لسلطات الدولة في فرض سيادتها على كامل إقليمها، مما يفقد مفهوم السيادة الكثير من معانيه، ويفرغه من محتواه، كما تشكل هذه الجرائم خطرا على النسيج الاجتماعي، لما تحدثه من اضطراب في نسق القيم، وشيوع الفوضى وانتهاك الحريات والحرمات، ناهيك عن التكلفة التي يتحملها المجتمع في سبيل تعقب هذه الجرائم، كما أنها تخلق أو تساعد في إيجاد بيئة ملائمة للإجرام، بحيث لا يعود بإمكان

[1] سامح أحمد، المرجع السابق، ص ص61-62.

[2] المرجع نفسه، ص ص62-64.

أفراد المجتمع تصريف أمور حياتهم اليومية دون خوف أو قلق، فمن الوارد جدا أن يتعرضوا باستمرار إلى المشاكل الناجمة عن المخدرات والاتجار بالبشر، والجريمة المنظمة وغيرها، كما أن الجرائم المعلوماتية تشكل خطرا على كيان الدولة ذاته، وعلى العملية الديمقراطية، بحيث تتوغل هذه الجرائم داخل سراديب الدول بشكل مخيف، وتمتلك مراكز قوة، فتصبح دولة داخل دولة، وقد يحدث في بعض الحالات أن تستغل الحكومات الاستبدادية الوضع لغرض فرض مزيد من القيود على الحريات العامة والشخصية، وهذا لا يخدم أبدا المسار الديمقراطي، كما أن الجرائم المعلوماتية تستهدف بالدرجة الأولى تحقيق أرباح مالية طائلة، بطرق غير مشروعة، وغالبا ما يتم إدماج هذه الأرباح في الأسواق بقصد تبييضها، وينعكس هذا الأمر سلبا على الاقتصاد، ويهدد المنافسة النزيهة بين المتعاملين الاقتصاديين، كما يشكل خطرا على البنوك والمؤسسات المالية والاقتصادية وكذا النظام الإداري للدولة.[1]

يقوم مجرمو الانترنت بانتحال الشخصيات والتغرير بالقصر، والتشهير وتشويه سمعة الأفراد والمؤسسات بل وحتى المجتمعات...مما حذا بالعالم للتحرك لمواجهة هذه الأخطار ووقعت ثلاثون دولة اتفاقية بودابست لمكافحة الإجرام عبر الانترنت، وشملت الاتفاقية عدة جوانب من بينها جرائم الإرهاب وعمليات تزوير بطاقات الوفاء والائتمان...

أما عن حجم أضرار هذه الجرائم فهي كبيرة ومتنوعة، وتشير التقارير المختلفة إلى أن حجم هذه الأضرار في بعض الدول قد بلغ مستويات قياسية، من ذلك تقرير برلماني أعدته لجنة العلوم والتكنولوجيا في مجلس اللوردات البريطاني يتحدث عن أضرار هذه الجرائم، ومنها خسارة البنوك البريطانية لمبلغ 67 مليون دولار عام 2006، وأعلن مكتب التحقيقات الفيدرالي الأمريكي سنة 2004 أن جرائم الكمبيوتر والانترنت تكلف الاقتصاد الأمريكي حوالي 67.2 مليار دولار سنويا.[2]

وفي الإمارات العربية المتحدة، قام سبعة أشخاص بالاحتيال على بنك دبي الإسلامي في الفترة الممتدة من 2004 إلى 2007، والاستيلاء على مبلغ فاق نصف مليار دولار، لتمويل

[1] سرحان حسن المعيني، المرجع السابق، ص ص29-30.

[2] سامح أحمد بلتاجي، المرجع السابق، ص78.

صفقات وهمية بمستندات مزورة، ومن المتهمين اثنان يعملان بالبنك أحدهما مدير لإدارة التمويل والآخر نائبه وهما من جنسية باكستانية.[1]

المطلب الثاني: مجرمو المعلوماتية.

يتم التطرق في هذا المطلب إلى تعريف المجرم المعلوماتي وصفاته (الفرع الأول)، أصناف مجرمي المعلوماتية ودوافعهم (الفرع الثاني).

الفرع الأول: تعريف المجرم المعلوماتي وصفاته.

المجرم هو كل من ارتكب فعلا يعد جريمة في نظر القانون، متى ثبت ذلك عن طريق سلطة قضائية مختصة، طبقا للإجراءات التي حددها المشرع في هذا الصدد، وجرائم الانترنت يرتكبها مجرمون متميزون عن المجرمين التقليديين الذين تطرقت إليهم كتب علم الإجرام المختلفة، ورغم ذلك لهم بعض الصفات المشتركة معهم، فالمجرم المعلوماتي هو كل شخص يمتلك علما وخبرة في مجال تقنيات الكمبيوتر وشبكة الانترنت، ويقوم باستغلال ذلك العلم الفني وخبرته التقنية لارتكاب جرائم معلوماتية، ولذلك يرى بعض الفقه أن فكرة المجرم المعلوماتي هي فكرة جديدة نسبيا على الفقه الجنائي.[2]

ينتمي المجرم المعلوماتي إلى وسط اجتماعي متميز، كما أنه على درجة عالية من العلم والمعرفة، ويتميز بذكاء فائق، وهو ما يميز بشكل عام ذوى الياقات البيضاء، وإن كان ليس من الضروري أن ينتمي المجرم المعلوماتي إلى مهنة يرتكب من خلالها الفعل الإجرامي، كما يتفق مجرم المعلوماتية مع ذوي الياقات البيضاء في أن الفاعل في الحالتين يبرر جريمته، بل إنه لا ينظر إلى سلوكه باعتباره جريمة أو فعلا يتنافى مع الأخلاق.[3]

وتعد المهارة المتطلبة لتنفيذ النشاط الإجرامي أبرز خصائص المجرم المعلوماتي، فتنفيذ الجريمة المعلوماتية بصفة عامة يتطلب قدرا من المهارة يتمتع بها الفاعل، والتي قد يكتسبها عن طريق الدراسة

---

[1] أ. د محمد قدري حسن عبد الرحمن، جرائم الاحتيال الإلكتروني، الفكر الشرطي، المجلد 20، العدد4، رقم 79، الشارقة، الإمارات العربية المتحدة 2011، ص79.

[2] سامح أحمد، المرجع السابق، ص80.

[3] نائلة فريد قورة، المرجع السابق، ص56.

المتخصصة في هذا المجال أو عن طريق الخبرة المكتسبة في مجال تكنولوجيا المعلومات، أو بمجرد التفاعل الاجتماعي مع الآخرين، غير أن ذلك لا يعني ضرورة أن يكون المجرم المعلوماتي على قدر كبير من العلم في هذا المجال أو أن تكون لديه خبرة كبيرة فيه، فالواقع العملي قد أثبت أن بعض أنجح مجرمي المعلوماتية لم يتلقوا المهارة اللازمة لارتكاب الجريمة عن طريق التعليم أو الخبرة المكتسبة من العمل في هذا المجال.

أما المعرفة فتتلخص في التعرف على كافة الظروف التي تحيط بالجريمة المراد تنفيذها، وإمكانيات نجاحها واحتمالات فشلها، فالجناة عادة يمهدون لارتكاب جرائمهم بالتعرف على المحيط الذي تدور فيه، لئلا يواجهوا بأشياء غير متوقعة من شأنها إفشال أفعالهم أو الكشف عنهم، وتميز المعرفة بمفهومها السابق مجرمي المعلوماتية، حيث يستطيع المجرم المعلوماتي أن يكون تصورا كاملا لجريمته، بسبب طبيعة مسرح الجريمة المعلوماتية الخاصة، بحيث يستطيع المجرم تنفيذ جريمته على أنظمة مماثلة لتلك التي يستهدفها وذلك قبل تنفيذ جريمته.[1]

أما الوسيلة فيراد بها الإمكانيات التي يتزود بها الفاعل لإتمام جريمته، ففيما يتعلق بالمجرم المعلوماتي فإن الوسائل المتطلبة للتلاعب بأنظمة الحاسبات الآلية هي في أغلب الحالات تتميز بالبساطة وبسهولة الحصول عليها، فالمجرم المعلوماتي له القدرة على الحصول على ما يحتاج إليه أو ابتكار الأساليب التي تقلل من الوسائل اللازمة لإتمام النشاط الإجرامي، والحقيقة أنه كلما كان نظام الحاسب الآلي الذي يحتوي على المعلومات المستهدفة غير مألوف، كانت الوسائل المتطلبة أكثر صعوبة في الحصول عليها، لاقتصارها على عدد قليل من الأفراد هم عادة القائمون على تشغيل النظام، وذلك على عكس الأنظمة الشائعة الاستعمال (برامج مايكروسوفت على سبيل المثال).[2]

أما السلطة فيقصد بها الحقوق أو المزايا التي يتمتع بها المجرم المعلوماتي والتي تمكنه من ارتكاب جريمته، فكثير من مجرمي المعلوماتية لديهم سلطة مباشرة أو غير مباشرة في مواجهة المعلومات محل الجريمة، وقد تتمثل هذه السلطة في الشفرة الخاصة بالدخول إلى النظام الذي يحتوي على المعلومات، والتي تعطي المجرم مزايا متعددة كفتح الملفات وقراءتها وكتابتها، ومحو أو تعديل ما بها من

[1] المرجع نفسه، ص57.

[2] نائلة فريد قورة، المرجع السابق، ص58.

معلومات، وقد تتمثل هذه السلطة في الحق في استعمال الحاسب الآلي أو إجراء بعض التعاملات أو مجرد الدخول إلى الأماكن التي تحتوي على أنظمة الحاسبات الآلية، كما قد تكون السلطة التي يتمتع بها المجرم غير حقيقية، كما في حالة استعمال شفرة الدخول الخاصة بشخص آخر.[1]

الفرع الثاني: أصناف مجرمي المعلوماتية ودوافعهم

عقدت وكالة حماية البرامج ندوة بشأن جرائم الانترنت، انتهت إلى تصنيف مجرمي الانترنت إلى أربع مجموعات وهي:

المجموعة الأولى: تعتبر من أكثر المجموعات رأفة وأقلها خطورة يتصدرها ثلة من الشباب يمتلكون قدرا لا بأس به من الخبرة المعلوماتية، وهوايتهم هي اللعب والتسلية بالكمبيوتر والانترنت.
المجموعة الثانية: وهي تماثل المجموعة السابقة، ولكن تتفوق عليها بأنها أكثر خبرة ومعرفة بعمليات البرمجة وتطبيقاتها.
المجموعة الثالثة: لها كفاءة المجموعة الثانية ذاتها، ولكنها أكثر خطورة إجرامية منها، لذا لا تكتفي بالمتابعة والملاحظة، بل تلجأ إلى أفعال الاعتداء عمدا.
المجموعة الرابعة: هي أكثر المجموعات خطورة وأشدها ضررا، ولها أهداف المجموعة السابقة، فهي تقوم بعمليات الإرهاب الإلكتروني ولكن باستخدام وسائل على قدر كبير من البراعة، كزرع برامج الفيروسات، والقنابل المنطقية خلسة.

وعلى هذا النحو يجوز تقسيم فئات مرتكبي جرائم الانترنت إلى:

– **هواة المعلوماتية:** ويسمون أيضا بصغار نوابغ المعلوماتية، هم من الشباب المولعين بالمعلوماتية والكمبيوتر،[2] لديهم قدر لا بأس به من المعلومات حول تقنيات الكمبيوتر والانترنت، وقد يتمكن بعضهم من اقتحام بعض الأنظمة البنكية والشركات والمؤسسات المالية، وعادة ما يمارس هؤلاء نشاطهم الإجرامي بهدف التسلية واللعب، وأهم سمات هذه الفئة أنهم يتبادلون المعلومات فيما بينهم

[1] المرجع نفسه، ص 58.

[2] القاضي وليد العاكوم، مفهوم وظاهرة الإجرام المعلوماتي، بحث مقدم إلى مؤتمر القانون والكمبيوتر والانترنت، المجلد الأول، الطبعة الثالثة 2004، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، ص12 وما بعدها.

عن طريق مجموعات الأخبار والنشرات الإعلانية الإلكترونية، ويطلعون بعضهم بعضا على مواطن الضعف والخلل في نظم المعلومات والشبكات.

وتتمثل خطورة هؤلاء الهواة في أنه يمكن بسهولة تحولهم إلى "هاكرز" وهم فئة أشد خطورة إجرامية، كما أنه قد يتم استغلالهم من قبل التنظيمات والعصابات واستعمالهم من أجل اختراق النظم الأمنية لنظم المعلومات الخاصة بالمؤسسات والهيئات الحكومية أو الخاصة.

ويتميز مجرمو هذه الفئة بالذكاء والنشاط، وأغلبهم من الذكور، وهم معتدلون في قيمهم الأخلاقية، ولديهم تبريرات ذاتية لأعمالهم الإجرامية.

ويرى جانب من الفقه أنه من الأجدى ألا يوصف هؤلاء الشباب بوصف"الإجرام" لأن أعمالهم ما هي إلا ميل للمغامرة والتحدي والرغبة في الاكتشاف،[1] وهذا لا يعني عدم متابعتهم الجزائية.

– **القراصنة:** لقي هذا المصطلح اتفاقا بين الفقه خلال فترة زمنية سابقة، لكن مدلوله تقلص كثيرا وأصبح لا يشمل سوى فئتين اثنتين هما "الهاكرز" و"الكراكرز".

لم يكن مصطلح "الهاكرز" في جذوره الأولى يحمل معنى سلبيا، بل كان يطلق على العلماء، وعلى كل شخص يمتلك قدرات فائقة في مجال التقنية، أما حديثا فتغير مدلوله ليشير إلى فئة من المجرمين الأذكياء يقومون باختراق مواقع الانترنت بما فيها مواقع التجارة الإلكترونية. والهاكرز متطفلون يتحدون إجراءات أمن النظم والشبكات، ولا تتوافر لديهم في الغالب دوافع حقد أو تخريب، وإنما يتطفلون من واقع التحدي وإثبات المقدرة والذكاء، لذا فهم ينفون عن أنفسهم تهمة ارتكاب الجرائم المعلوماتية بأن النية الإجرامية لم تتوافر لديهم، أي عدم توافر الركن المعنوي للجريمة مما يعني عدم توافر الجريمة بالأساس.

[1] عبد الفتاح بيومي حجازي، الإثبات الجنائي في جرائم الكمبيوتر والانترنت، دار الكتب القانونية، المحلة الكبرى، القاهرة 2007، ص76 وما بعدها.

وتطور مصطلح "الهاكرز" إلى مصطلح جديد هو "الكراكرز" ويعني "الهاكر سيء النية" وهو أشد خطورة من "الهاكر" لأن لديه كفاءة عالية وسوء نية، وأحيانا يسمى "الهاكر" "بالعنكبوتي" لأنه يختفي في الظلام تاركا آثارا سيئة بسبب مروره.

ويتميز القراصنة عموما بعدم ميلهم للعمل الفردي، وإيثارهم العمل في مجموعات، مما يزيد من مدى خطورتهم، وهم يشكلون أندية مثل نادي "كلودو" بفرنسا.

– **المخربون أو الحاقدون:** هاته الفئة من مجرمي المعلوماتية لا يرتكب أفرادها الجرائم بدافع إثبات القدرات والإمكانيات في مجال استخدام الكمبيوتر والانترنت، ولا من أجل تحقيق مكاسب أو أرباح مالية، وإنما دافعهم لارتكاب هذه الجرائم هو الحقد أو الغضب، والرغبة في الانتقام أو الثأر من شخص أو مؤسسة أو دولة ما.

ويغلب على أنشطة هذه الفئة من مجرمي المعلوماتية من الناحية التقنية، استخدام تقنية زراعة الفيروسات، والبرامج الضارة، وتخريب النظام وإتلافه كليا أو جزئيا، ويقوم البعض من هؤلاء المجرمين بإرسال رسائل البريد الإلكتروني محملة بالفيروسات إلى أنظمة المعلومات لأي شركة أو شخص مما يؤدي إلى تخريب الأنظمة والمعلومات المخزنة في أجهزة الكمبيوتر.

وبالرغم من أن فئة المخربين أو الحاقدين تعتبر أقل مجرمي الانترنت خطورة لأن قدرات كثير من مجرميها محدودة في مجال التقنية، إلا أن ذلك لا يمنع أن تكون الأضرار الناجمة عن أنشطة بعضهم جسيمة.[1]

– **المجرمون المحترفون:** يعد المجرمون المحترفون أخطر مجرمي الانترنت، لنبوغهم الشديد في مجال تقنيات وبرمجيات وعلوم الكمبيوتر والانترنت، وغالبا ما يكون الهدف الأساسي لهؤلاء تحقيق مكاسب مادية، لذا فإن لديهم دوما عنصر العمد في ارتكاب الجرائم، وتنصب معظم جرائمهم على شركات تحويل الأموال، والتلاعب بحسابات البنوك وفواتير الكهرباء والغاز وتزوير بطاقات الائتمان.[2]

[1] سامح أحمد بلتاجي، المرجع السابق، ص90.

[2] بيومي حجازي، المرجع السابق، ص82.

وينظر الناس إلى كثير من المنتمين إلى هذه الفئة على أنهم مستخدمون مثاليون، فغالبيتهم يشغلون مراكز قيادية هامة، ويتمتعون بثقة كبيرة في مجال عملهم، وهذا ما يزيد من خطورتهم، بالإضافة إلى غموض شخصياتهم، وقيامهم المستمر بتغيير وظائفهم، فهم مجرمون من ذوي الياقات البيضاء،[1] وهم لا يبالون إلا بما يعود عليهم بالنفع المادي، ولا يستشعرون أن سلوكاتهم تستحق العقاب، وتزداد خطورة هؤلاء المجرمين عندما يستخدمون من قبل جماعات إرهابية أو من قبل جهات خارجية للتجسس على الدول والشركات.

خلاصة القول أن الباعث وراء ارتكاب الجريمة المعلوماتية، لا يختلف في كثير من الأحيان عن الباعث لارتكاب غيرها من الجرائم الأخرى، فالرغبة في تحقيق الربح المادي بطريق غير مشروع يظل الباعث الأول وراء ارتكاب الجريمة المعلوماتية، ثم يأتي بعد ذلك مجرد الرغبة في قهر نظام الحاسب وتخطي حواجز الحماية المضروبة حوله. وأخيرا الانتقام من رب العمل أو أحد الزملاء، والحقيقة أنه أيا ما كان الباعث وراء ارتكاب الجريمة المعلوماتية فإنه يوجد شعور دائم لدى مرتكب الفعل بأن ما يقوم به لا يدخل ضمن نطاق الجرائم، أو بتعبير آخر لا يمكن أن يتصف بأنه غير أخلاقي، وخاصة في الحالات التي يقف فيها السلوك عند حد قهر نظام الحاسب الآلي وتخطي الحماية المضروبة حوله، حيث يفرق مرتكبو هذه الجرائم بين الإضرار بالأشخاص الأمر الذي يعدونه غاية في "اللاأخلاقية"، وبالتالي ينبغي تجنبه والإعراض عنه، وقدح كل من يقوم به، وبين الإضرار بمؤسسة أو جهة في استطاعتها اقتصاديا تحمل نتائج تلاعبهم، وهو ما يطلق عليه أعراض "روبن هود".[2]

[1] سامح أحمد بلتاجي، المرجع السابق، ص91.

[2] نائلة فريد قورة، المرجع السابق، ص ص58-59.

الباب الأول: الجرائم الواقعة على التجارة الإلكترونية.

يقتضي تحقيق الحماية الجزائية للتجارة الالكترونية، التطرق إلى أبرز الجرائم التي يمكن أن ترتكب على هذه التجارة، وتبيان أركانها، ولذلك يتم تقسيم هذا الباب إلى فصلين، يتناول الفصل الأول الحماية الجزائية لمواقع التجارة الالكترونية على الانترنت وغيرها من الشبكات ومحتوياتها، أما الفصل الثاني فيتناول حماية ما انفك يطلق عليه جانب من الفقه "بالمستهلك الإلكتروني".

الفصل الأول: الحماية الجزائية لمواقع التجارة لإلكترونية على الانترنت ومحتوياتها.

الموقع الإلكتروني فكرة جديدة ارتبط ظهورها بظهور الانترنت وزيادة التبادل التجاري عبرها، وما تبع ذلك من معاملات تجارية إلكترونية مختلفة؛ ويحتوي الموقع الإلكتروني على العديد من المحتويات تعتبر وسيلة فعالة للإعلان عن البضائع والخدمات، ويتضمن تعريفا بصاحب الموقع والعديد من البيانات المتصلة بذلك، مما يجعل للموقع أهمية بالغة بالنسبة للتجارة الإلكترونية، وهذا يقتضي تحقيق حماية قانونية وتقنية كافية له سواء أكان ذلك لمحتواه أو لاسمه،[1] وبناء عليه، يتم معالجة هذا الفصل من خلال التطرق إلى الحماية الجزائية ضد الدخول غير المشروع لمواقع التجارة الالكترونية، من خلال تجريم الاعتداء على نظم المعالجة الآلية للمعطيات (المبحث الأول)، وحماية حقوق الملكية الفكرية للتجارة الالكترونية (المبحث الثاني).

المبحث الأول: تجريم الاعتداء على نظم المعالجة الآلية للمعطيات.

أدرك المشرع في التقنين المقارن خطورة أفعال الاعتداء على أجهزة الحاسب الآلي أو الكمبيوتر، وبرامجها، وقواعد البيانات، فبادر إلى التدخل لتوفير حماية قانونية كافية لها، مستعملا وسائل القانون الجزائي باعتباره الأكثر قدرة على تحقيق المطلوب.[2]

---

[1] د. فاتن حسين حوى، المواقع الإلكترونية وحقوق الملكية الفكرية، دار الثقافة للنشر والتوزيع عمان، الأردن، ط2010، ص51.

[2] صدر في الولايات المتحدة القانون الفيدرالي في شأن الاعتداء على الكمبيوتر واستغلاله في عام 1984 وعدل في أعوام 1986 و 1994 و1996 ورد في الفصل 1030 منه نصوص خاصة تجرم الاعتداء على الكمبيوتر والمتعلقة بأنشطة متصلة بالكمبيوتر.

ويعاقب هذا الفصل على الأفعال أي شخص يدخل عمدا على جهاز حاسب آلي بدون تصريح أو يحصل- بأي وسيلة كانت متجاوزا حدود التصريح الممنوح له – على معلومات لا تجيز الحكومة الأمريكية الكشف عنها لأمور تتعلق بالدفاع الوطني أو العلاقات الخارجية، أو أي بيانات سرية من ذلك ما حدد في الفقرة (ي) من الفصل الثاني من قانون الطاقة النووية الصادر سنة 1954، إذا اتجهت إرادة الجاني إلى ارتكاب أو توافر الاعتقاد أن مثل

هذه المعلومات ستستخدم للمساس بأمن ومصالح الولايات المتحدة الأمريكية، أو بمصالح أي دولة أجنبية، كما يعاقب القانون كل من يقوم عمدا بالدخول على جهاز حاسب آلي دون ترخيص، أو بتجاوز الترخيص الممنوح له ويحصل على معلومات موجودة في سجل اقتصادي يخص مؤسسة مالية أو يخص مانح بطاقات مالية، أو المعلومات الموجودة في تقرير يتعلق بالمستهلكين.

يعاقب القانون أيضا على الدخول العمدي على البيانات الموجودة بأجهزة الكمبيوتر الخاصة بالوكالات والجهات والتي يقتصر استعمالها على حكومة الولايات المتحدة الأمريكية، وإذا كان الاستعمال لا يقتصر كلية على حكومة الولايات المتحدة الأمريكية ولكنه يستعمل لمصلحتها وكان من شأن الدخول على الكمبيوتر أن يؤثر في هذا الاستعمال.

ويعاقب المشرع الأمريكي كذلك كل من يدخل على جهاز للكمبيوتر يستخدم في التجارة أو الاتصال بين الولايات ويقوم عمدا بنقل لبرنامج أو معلومة أو كود لكمبيوتر أو نظام للكمبيوتر.

ويعاقب المشرع الأمريكي كل من يمنع أو يحرم أو يتسبب في منع أو حرمان الغير من استعمال كمبيوتر أو خدمات كمبيوتر أو نظام أو شبكة أو معلومات أو بيانات أو برنامج.

ويعاقب القانون الأمريكي كذلك على نقل أي مكونات لبرامج أو معلومات أو كود أو أمر دون موافقة من المسؤولين على الكمبيوتر المستقبل للبرنامج أو المعلومات أو الكود أو الأمر إذا أدى هذا النقل إلى خسائر لشخص أو أكثر تبلغ ألف دولار أو أكثر خلال فترة سنة من ارتكاب الفعل أو إذا أدت إلى تعديل أو إفساد كلي أو جزئي لكشف أو تقرير طبي أو علاج طبي أو الرعاية الصحية لشخص أو أكثر.

فرض المشرع الأمريكي عقوبة على القيام بنقل برنامج أو معلومات أو كود أو أمر بطريق الكمبيوتر لجهاز يستخدم في التجارة أو الاتصال بين الولايات، ويشكل الفعل خطورة أن النقل أضر أو تسبب في الإضرار لكمبيوتر أو شبكة أو معلومة أو بيان أو برنامج، وكان ذلك دون تصريح من المسئولين عن النظام الذي نقل إليه البرنامج أو المعلومة أو الكود أو الأمر وتسبب في خسائر تقدر بألف دولار أو أكثر خلال فترة سنة أو عدل أو عطل كليا أو جزئيا التقارير الطبية.

ويعاقب القانون كذلك على غش كلمات المرور بما يسمح بالدخول على نظام للكمبيوتر دون تصريح إذا كان من شأن ذلك الإضرار بالتجارة بين الولايات أو بالتجارة الخارجية.

ولقد قرر المشرع الأمريكي عقوبات مشددة للجرائم المشار إليها والشروع فيها.

ومع ذلك فقد كشف التقرير الصادر عن لجنة عمل رئيس الولايات المتحدة الأمريكية في شأن السلوك غير المشروع على الانترنت في مارس 2000 أن القانون ينطوي على الكثير من الغموض والقصور بحيث يمكن للمجرمين تلافي تطبيق القانون عليهم باستخدام حاسبات وشبكات تقع خارج الولايات المتحدة الأمريكية، كما يمكن لمجرمي الكمبيوتر من خارج الولايات المتحدة الأمريكية استخدام الأنظمة الموجودة بالدولة للاعتداء على حاسبات تقع في دول أخرى. مدحت عبد الحليم رمضان، المرجع السابق،ص ص41-44.

أما بالنسبة لاتفاقية بودابست، تلزم م2 من الاتفاقية والخاصة بالولوج غير القانوني، كل طرف بتبني الإجراءات التشريعية المناسبة أو أية إجراءات أخرى ضرورية بقصد اعتبار فعل الولوج العمدي إلى كل أو جزء من النظام المعلوماتي، جريمة وفقا للقانون الداخلي لكل دولة، كما يجوز لكل طرف أن يشترط أن ترتكب الجريمة من خلال انتهاك إجراءات الأمن، بقصد الحصول على بيانات الحاسب الآلي، أو أي قصد إجرامي آخر، أو أن ترتكب الجريمة في حاسب آلي يكون متصلا عن بعد بحاسب آخر، ويعتبر التقرير التفسيري الخاص باتفاقية بودابست جريمة الولوج غير القانوني الجريمة الرئيسة التي تنطوي على تهديد واعتداء على أمن سرية وسلامة النظم وأمنها، وعليه فإن مجرد الدخول غير المرخص به يعتبر في حد ذاته جريمة.

للدخول غير المصرح به أو غير القانوني أو غير المشروع مجموعة من الصور من أهمها: اختراق النظام كله أو جزء منه، ويستوي أن يكون الجزء ماديا أو برامج جزئية ترتبط ببرامج أخرى لتنفيذ وظيفة معينة، أو بيانات مخزنة في نظام التنصيب، أو بيانات تتعلق بالمرور أو بالمحتوى، ويضيف التقرير إلى أن جريمة الدخول (الولوج) غير القانوني لا تقوم إلا إذا كان فعل الولوج بدون حق.

أشار التقرير إلى أن هناك العديد من التشريعات الوطنية سبق وأن تضمنت نصوصا متعلقة بالجرائم المرتبطة بالقرصنة، إلا أن نطاقها وكذا العناصر المكونة لها متنوعة ومتباينة، كما أن المدخل العام للعقاب في العبارة الأولى من المادة الثانية لا يخلو من تنازع أو اختلاف، وغالبا ما تتعدد المواقف حينما لا يترتب عن الدخول غير المشروع إلى النظام المعلوماتي مخاطر أو حينما تؤدي عمليات القرصنة إلى اكتشاف نقاط ضعف في أمن النظم المعلوماتية، ويمكن انطلاقا من التقرير التفسيري، استخلاص أن أطراف الاتفاقية بإمكانهم تبني المدخل العام، وتجريم القرصنة دون قيد أو شرط، استنادا إلى الفقرة الأولى من المادة الثانية من الاتفاقية، إذا ارتكبت الجريمة انتهاكا للإجراءات الأمنية، أو بنية الحصول على بيانات معلوماتية، أو أية نية إجرامية تبرر قيام

تظهر الحاجة إلى الحماية الجزائية للمعطيات، أو المعلومات المعالجة آليا عن المعلومات التي تحتويها الملفات الورقية، من خصوصيتها المتمثلة في ضعفها وأهميتها، فالمعلومات (البيانات) المعالجة آليا ضعيفة داخل النظام، مقارنة بالمعلومات داخل الملفات الورقية التي يمكن إخفاؤها بسهولة مقارنة بالمعلومات داخل النظام، كما أن المعلومات المعالجة آليا (المعطيات) تتميز بالضخامة والتنوع، ومنها ما يتعلق بالحياة الخاصة للأفراد، هذه الاعتبارات وغيرها دعت المشرع في القوانين المقارنة إلى استحداث صور من التجريم حماية للمعطيات، لا يوجد مثيل لها بالنسبة للمعلومات المسجلة داخل الملفات الورقية.[1]

ولا يخرج الاعتداء على مواقع التجارة الإلكترونية عبر الانترنت عن كونه أحد تطبيقات الاعتداء على أجهزة الكمبيوتر الذي يستخدم في إعداد هذه المواقع وبرامجها المختلفة.[2]

المسؤولية الجزائية، أو باشتراط أن يتم ارتكاب الجريمة في نطاق معلوماتي متصل عن بعد بنظام معلوماتي آخر، وهذا الخيار الأخير يسمح لأطراف الاتفاقية باستبعاد الحالة التي يكون فيها الجاني قد وصل ماديا إلى جهاز حاسب مستقل، دون المرور بواسطة حاسب أو نظام معلوماتي آخر.

نصت م5 من اتفاقية بودابست على: "يجب على كل طرف أن يتبنى الإجراءات التشريعية وأية إجراءات أخرى ويرى أنها ضرورية لتجريم، تبعا لقانونه المحلي، الإعاقة الخطيرة،إذا تم ذلك عمدا، وبدون حق، لوظيفة نظام الحاسب، عن طريق إدخال أو نقل أو إضرار أو محو أو تعطيل أو إتلاف أو طمس البيانات المعلوماتية.

ويبدو أن هذا النص من الاتفاقية يهدف إلى تجريم الإعاقة العمدية للاستخدام الشرعي للنظم المعلوماتية، والتي تعتبر في كثير من الأحيان نتيجة للولوج غير القانوني لأي نظام معلوماتي. ومصطلح الإعاقة يرتبط بالأفعال التي تحمل اعتداءا على حسن تشغيل النظم المعلوماتية، وهذه الإعاقة يجب أن تكون ناجمة عن الإدخال أو النقل أو الإضرار أو المحو أو الإتلاف أو طمس البيانات المعلوماتية.

وبناء عليه، فإن إعاقة النظام الخاص بموقع التجارة الإلكترونية قد يقع بإحدى المذكورة سلفا، بحيث أن أي موقع الكتروني تجاري يتضمن مجموعة من البيانات المعلوماتية سواء تلك المرتبطة بمواصفات السلع أو الخدمات، أو بيانات خاصة بصاحب المشروع أو بيانات أخرى تتطلبها عمليات البيع والشراء عبر شبكة الانترنت.

يشير التقرير التفسيري إلى أن الإعاقة الجسيمة للنظام المعلوماتي، تتحقق عندما تكون البيانات المرسلة من الحجم أو التواتر ما يحمل ضررا جسيما لقدرة المالك والمشغل بالنسبة لاستخدام الجهاز أو الاتصال بالأجهزة الأخرى، ومثال ذلك البرامج التي تحمل اعتداء على النظم، والتي تأخذ شكل الامتناع عن الخدمة أو الشفرات العدوانية كالفيروسات التي تمنح أو تبطئ بشكل ملموس عمل الجهاز، أو البرامج التي ترسل قدرا هائلا من البريد الالكتروني إلى مرسل إليه بهدف شل وظائف اتصال نظام الحاسب.

ويشير نص المادة 5 إلى أن الإعاقة يجب أن تكون بدون حق، بحيث إن الأمر يتعلق بأنشطة اختبار أمن نظام الحاسب الآلي، أو حماية النظام والمصرح بها من المالك أو القائم بتشغيله، أو عند إعادة تنظيم نظام تشغيل حاسب، فكل هذه الأنشطة غير شرعية، يعاقب عليها استنادا على هذه المادة. وتركت م5 من الاتفاقية المذكورة للدول الأطراف مسألة تحديد الحالة التي يكون فيها عمل النظام معاقا بشكل كلي أو جزئي، مؤقت أو دائم، حيث يمكن معرفة ما إذا كانت الإعاقة تتطلب جزاء جنائيا أو مجرد جزاء إداري. والمادة ذاتها تشترط لقيام هذه الجريمة توافر القصد العمدي، بحيث تتوافر لدى مرتكب الجريمة نية إحداث إعاقة جسيمة. أمين أعزان، المرجع السابق،ص ص88-90.

[1] غنام محمد غنام، دور قانون العقوبات في مكافحة جرائم الكمبيوتر والانترنت، دار الفكر والقانون، المنصورة، مصر 2013، ص124.

[2] مدحت عبد الحليم رمضان، المرجع السابق، ص37.

لقد أفرزت الوسائل الحديثة المتعلقة بالمعلومات والاتصالات منذ أكثر من ثلاثة عقود خلت، صورا جديدة من الاعتداءات لم تكن مألوفة من قبل، وقد تدخل المشرع لتجريمها، ففي فرنسا أصدر المشرع القانون المتعلق بالغش المعلوماتي أو الجريمة المعلوماتية "la fraude informatique"، المسمى "Godfrain" رقم 88-19 في 5 يناير 1988 جرم العديد من الأفعال المرتبطة في تلك الفترة باستعمال "المينتال"، وهذه القواعد القانونية قابلة حاليا للتطبيق على شبكة الانترنت ومختلف وسائل الاتصال الحديثة، ولقد تم إدخال هذه القواعد القانونية ضمن قانون العقوبات الفرنسي لسنة 1994، لتتمم بالقانون رقم 575-2004 لسنة 2004 المسمى قانون الثقة في الاقتصاد الرقمي المعروف اختصارا ب: "LCEN" والذي أخذ في الحسبان توجيهين أوربيين، فشدد العقوبات وأوجد جنحة جديدة هي حيازة أو وضع أي برنامج أو معطى "donnée" هدفه ارتكاب جريمة من الجرائم المنصوص عليها في المواد 323-1 إلى 323-3 من قانون العقوبات الفرنسي.[1]

والدخول غير المشروع إلى مواقع التجارة الإلكترونية عبارة عن صور لجرائم عامة يطلق عليها "جرائم الاعتداء على نظم المعالجة الآلية للمعطيات"[2] سواء تعلق الأمر بالتجارة الالكترونية أو غيرها، وصور هذه الجرائم هي: الدخول غير المشروع على نظم معالجة المعطيات، إعاقة أو تحريف تشغيل نظم معالجة البيانات، والتلاعب في بيانات نظم المعالجة الآلية للمعطيات.[3]

وقبل التطرق إلى كل جريمة من هذه الجرائم على حدة، يحسن التعرض إلى الأحكام المشتركة بين جرائم الاعتداء على نظم المعالجة الآلية للمعطيات.

[1] Béatrice Clément et autres, fiches de droit pénal spécial, ellipses édition, Paris 2012, p266.
[2] Des atteintes aux systèmes de traitement automatisé de données.
[3] عبد الفتاح بيومي حجازي، التجارة الالكترونية وحمايتها القانونية، الكتاب الثاني، الحماية الجنائية لنظام التجارة الالكترونية، دار الكتب القانونية، المحلة الكبرى، مصر 2007، ص14.

المطلب الأول: الأحكام المشتركة بين جرائم الاعتداء على نظم المعالجة الآلية للمعطيات.

نص قانون العقوبات الفرنسي على جرائم الاعتداء على نظم المعالجة الآلية للمعطيات في المواد 323-1 إلى 323-7.

في الجزائر، قام المشرع بتعديل قانون العقوبات لتوفير الحماية الجزائية للأنظمة المعلوماتية،[1] وأساليب المعالجة الآلية للمعطيات، وكان ذلك بموجب القانون رقم 15/04 المؤرخ في 10 نوفمبر 2004، الذي أضاف القسم السابع المكرر تحت مسمى"المساس بأنظمة المعالجة الآلية للمعطيات"، تضمن ثماني مواد: 394 مكرر إلى 394مكرر7.

الفرع الأول: مفهوم نظام المعالجة الآلية للمعطيات.

نظام المعالجة الآلية للمعطيات (STAD) هو الشرط الأول الذي يلزم تحققه قبل البحث عما إذا كان هنالك اعتداء على قواعد بيانات التجارة الالكترونية أم لا؛ وكان مجلس الشيوخ الفرنسي قد اقترح تعريفا لنظام المعالجة الآلية للمعطيات عند طرح القانون رقم 88-19 لسنة 1988، بأنه "كل مركب يتكون من وحدة أو مجموعة وحدات معالجة، والتي تتكون كل منها من الذاكرة والبرامج والمعطيات، وأجهزة الإدخال والإخراج، وأجهزة الربط، والتي يربط بينها مجموعة من العلاقات التي عن طريقها يتم تحقيق نتيجة معينة وهي معالجة المعطيات، على أن يكون هدا المركب خاضعا لنظام المعالجة الفنية".[2]

والملاحظ على هذا التعريف أنه أشار للعناصر المادية والمعنوية التي يتكون منها المركب، وذكرها على سبيل المثال لا الحصر.[3]

---

[1] وقد عرفت المادة 2/ب من القانون رقم 04/09 المؤرخ في 05 أوت 2009 والمتضمن القواعد الخاصة للوقاية بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، المقصود بالمنظومة المعلوماتية بأنها:" أي نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض، أو المرتبطة، يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين". ينظر: العدد 47 من الجريدة الرسمية لسنة 2009.

[2] بيومي حجازي، المرجع السابق، ص21. ويراجع أيضا:

Renaud Salomon, droit pénal des affaires, LexisNexis Litec, Paris2009,p213.

[3] بيومي حجازي، المرجع السابق، ص22.

وأكدت اتفاقية بودابست لسنة 2001 أن النظام المعلوماتي عبارة عن جهاز يتكون من مكونات مادية ومكونات منطقية، وذلك بغية المعالجة الآلية للبيانات الرقمية، ويشمل وسائل لإدخال وإخراج وتخزين البيانات.[1]

وعرفت م5/2 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات سالفة الذكر النظام المعلوماتي بأنه: "مجموعة برامج وأدوات معدة لمعالجة وإدارة البيانات والمعلومات"، كما عرفت المادة ذاتها في الفقرة الثالثة البيانات بأنها: "كل ما يمكن تخزينه ومعالجته وتوليده ونقله بواسطة تقنية المعلومات، كالأرقام والحروف والرموز وما إلى ذلك..." كما عرفت المادة ذاتها في الفقرة الأولى تقنية المعلومات بأنها: "أية وسيلة مادية أو معنوية أو مجموعة وسائل مترابطة أو غير مترابطة تستعمل لتخزين المعلومات وترتيبها وتنظيمها واسترجاعها ومعالجتها وتطويرها وتبادلها وفقا للأوامر والتعليمات المخزنة بها، ويشمل ذلك جميع المدخلات والمخرجات المرتبطة بها سلكيا أو لا سلكيا في نظام أو شبكة".

حسب الأحكام القضائية الفرنسية يجوز تعريف أنظمة المعالجة الآلية للمعطيات على أنها آلة، جهاز كمبيوتر (حاسب آلي)، هاتف، شبكة محلية للمؤسسة (إذن مجموعة حاسبات آلية تسمى نظام معلومات)، خدمة، محرك بحث، برنامج يضمن التشغيل (logiciel).[2]

وعرفت م3/2 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات سالفة الذكر البيانات "المعطيات" بأنها كل ما يمكن تخزينه ومعالجته وتوليده ونقله بواسطة تقنية المعلومات، كالأرقام والحروف والرموز وما إليها.

نظرا لقيمة نظم المعلومات، جرم المشرع التعدي عليها، بأية صورة كانت، سواء بتدميرها، أو تعييبها، أو إعاقة عملها، فضرر ذلك يفوق ضرر إتلاف المعدات المادية الخاصة بنظم المعلومات.[3]

وثار سؤال في شأن جرائم التعدي على نظم معالجة البيانات مفاده: "هل يشترط لقيام الجريمة أن تكون هنالك حماية فنية لذلك النظام، من قبل صاحبه أو من له الحق فيه؟"

---

[1] أمين أعزان، المرجع السابق، ص76.

[2] Béatrice Clément et autres, op cit, p267.

[3] بيومي حجازي، المرجع السابق، ص22.

رأى جانب من الفقه الفرنسي ضرورة اشتراط وجود نظام أمان، كشرط مفترض لقيام الجرائم المتعلقة بنظم المعلوماتية، لأن العدالة تقتضي عدم العقاب على فعل اعتداء على حق لم يحتط له صاحبه، كما أن التسليم بغير هذا، يعني توسعا في مجال التجريم، فكل دخول غير مشروع يعد جريمة، وذلك أمر غير منطقي، حسب وجهة نظرهم.[1]

إلا أن الرأي الغالب في الفقه الفرنسي لا يشترط وجود نظام أمان لقيام هذه الجرائم، لأن النصوص الواردة في هذا الشأن لم تتضمن شرط الحماية الفنية، ولا يجوز تقييد النص المطلق،[2] ونظام الأمن ليس له إلا دور واحد، وهو إثبات سوء نية من قام بانتهاك النظام والدخول غير المشروع إليه، في إطار إثبات القصد الجنائي، وهذه مسألة أخرى.[3]

وتزكي أحكام القضاء الفرنسي هذا الرأي، حيث أنها لم تشترط لقيام الجريمة وجود حماية فنية.[4]

الفرع الثاني: المصلحة المحمية في جرائم نظم المعلومات.

المصلحة عبارة عن رابطة بين شخص ومال، بمقتضاها يستطيع الشخص أن يشبع حاجاته من المال، والمصلحة هي محل الحماية القانونية، والاعتداءُ عليها يتمثل في إهدارها أو تهديدها بخطر.

وفيما يخص نظم المعلومات، فمن التشريعات من ركزت على فكرة الملكية، ومنها من ركزت على فكرة سلامة المعطيات، ومنها من تحمي سريتها، ومنها من حاولت الجمع بين ذلك كله،[5] حيث أن هناك اتجاها يحمي معطيات الكمبيوتر وبرامجه في إطار حماية الملكية الخاصة، وهناك اتجاه آخر يحمي سلامة معطيات الكمبيوتر مهما كانت طبيعة النشاط الإجرامي الذي تتعرض له هذه المعطيات، كأن يجرم التلاعب بالمعطيات ويعتبره شكلا من أشكال التزوير، وهناك اتجاه ثالث

---

[1] المرجع نفسه، ص24.

[2] المرجع نفسه، ص24.

[3] المرجع نفسه، ص23.

[4] أمين أعزان، المرجع السابق، ص79.

[5] محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، دار الجامعة الجديدة، الأزاريطة، الإسكندرية، مصر 2007، ص80

يركز على المعلومات ذاتها، خاصة المتعلقة بالأشخاص، فيهدف إلى حماية سرية هذه المعلومات، عن طريق تجريم الدخول غير المصرح به إلى نظم الكمبيوتر، وهناك اتجاه رابع يجمع بين أكثر من اتجاه من الاتجاهات السابقة، ويهدف إلى حماية مصالح متعددة، عن طريق مجموعة من النصوص المتكاملة فيما بينها.[1]

إذا ألقينا نظرة في نصوص كلا من قانون العقوبات الفرنسي، وقانون العقوبات الجزائري، وجدنا أن هذه النصوص تعمل على حماية ثلاث مصالح رئيسة وهي: سرية المعطيات، سلامتها أو تكاملها، وإتاحتها؛ فلحماية سرية المعطيات قام المشرع بتجريم الدخول غير المشروع إلى أنظمة المعالجة الآلية للمعطيات، ولحماية سلامة المعطيات أو تكاملها جرم التلاعب بالمعطيات إدخالا وإزالة وتعديلا، والنص على هذه الجرائم يحمي المعطيات في إتاحتها ووفرتها.[2]

الفرع الثالث: العقوبات التكميلية.

العقوبات التكميلية هي عقوبات غير أصلية، وهي تلك العقوبات التي يوقعها القاضي وجوبا أو جوازا بالإضافة إلى العقوبة الأصلية، فلا يملك الحكم بها بمفردها.

من الأحكام المشتركة بين جرائم الاعتداء على أنظمة المعالجة الآلية للمعطيات، العقوبات التكميلية التي يحكم بها إلى جانب العقوبات الأصلية لكل جريمة من الجرائم المذكورة.

وقد نص المشرع الجزائري في م394 مكرر6 ق ع على نوعين من العقوبات التكميلية هما المصادرة والغلق،[3] ويبدو من خلال نص هذه المادة أن العقوبة التكميلية هنا وجوبية، حيث يظهر من خلال صياغة نص المادة أنها تجبر القاضي على الحكم بها مع العقوبة الأصلية، ولا تخيره في ذلك.[4]

---

[1] المرجع نفسه، ص82.

[2] المرجع نفسه، ص83.

[3] تنص م394 مكرر6 من ق ع على: "مع الاحتفاظ بحقوق الغير حسن النية، يحكم بمصادرة الأجهزة والبرامج والوسائل المستخدمة مع إغلاق المواقع التي تكون محلا لجريمة من الجرائم المعاقب عليها وفقا لهذا القسم، علاوة على إغلاق المحل أو مكان الاستغلال إذا كانت الجريمة قد ارتكبت بعلم مالكها".

[4] محمد خليفة، المرجع السابق، ص120.

وقد استخدم المشرع الجزائري عند تطرقه للمصادرة لفظ "الوسائل المستخدمة في ارتكاب الجريمة"، وهو مصطلح عام، والحكمة من ذلك أن يستوعب أية وسيلة تستجد في ارتكاب جرائم المعطيات، مهما كانت طبيعة هذه الوسيلة، وسواء كانت معدة خصيصا لارتكاب هذه الجرائم أم لا.

ولا يجب أن تمس المصادرة بحقوق الغير حسن النية،[1] ما دامت نيته كانت حسنة وقت ارتكاب الجريمة أو وقت نشأة حقه حسب الأحوال، ويترتب على ذلك أنه لا يجوز مصادرة الأشياء المملوكة للغير حسن النية، حتى ولو كان للجاني حق عيني عليها، أما إذا كان للغير حسن النية حق عيني على هذه الأشياء جازت مصادرتها محملة بحقوق الغير.[2]

العقوبة التكميلية الثانية التي نصت عليها م394 مكرر6 هي الغلق، وحسب نص المادة المذكورة، يتم غلق المواقع التي تكون محلا لإحدى الجرائم المنصوص عليها، وكذا غلق محل أو مكان الاستغلال إذا كانت الجريمة قد ارتكبت بعلم مالكها، ويبدو أن المشرع قد استخدم عنصر العلم وهو أحد مكوني الركن المعنوي للتعبير عن القصد الجنائي.

والمواقع التي يقصدها المشرع الجزائري، والتي تكون محلا للغلق هي تلك المواقع التي استعملت في ارتكاب الجريمة، كالمواقع التي تقدم خدمات تتيح الولوج غير المصرح به لمختلف أنظمة المعطيات، أو التلاعب بهذه الأنظمة، أو المواقع التي تقوم بتعليم كيفية تصميم المعطيات غير المشروعة وتوفرها وتنشرها وتتاجر فيها، ولذلك كان من الأحسن أن يستعمل المشرع الجزائري عبارة "المواقع التي تستعمل في ارتكاب الجريمة"، بدل عبارة "المواقع التي تكون محلا لجريمة من الجرائم"، لأن هذه المواقع معتدى عليها، فهي ضحية، ولا يتصور أن تطال العقوبات الضحايا.[3]

شأنها شأن عقوبة المصادرة، لا تطال عقوبة الغلق، الغير حسن النية، ولم يحدد نص م394 مكرر6 مدة الغلق، وعليه وحسب القواعد العامة، يجوز أن تكون المدة مؤبدة، أو مؤقتة (م16 مكرر1 ق ع).

---

[1] لا تقتصر هذه الحقوق على الملكية، بل تمتد لتشمل أي حق عيني على الشيء، كحق الانتفاع أو الرهن. المرجع السابق، ص120.

[2] المرجع نفسه،ص ص121-122.

[3] محمد خليفة، المرجع السابق، ص123.

أما المشرع الفرنسي فقد نص في م5/323 ق ع ف علاوة على الغلق والمصادرة على مجموعة من العقوبات التكميلية، كالحرمان من الحقوق السياسية والمدنية، و الحرمان من تولي الوظائف العامة، أو أي نشاط مهني أو اجتماعي...[1]

والملاحظ أن هذه العقوبات التكميلية التي ذكرها نص م5/323 ق ع ف، قد اعتمدها المشرع الجزائري في تعديل قانون العقوبات لسنة 2006[2] في المادة 9 كالآتي:

1- الحجر القانوني،[3]
2- الحرمان من ممارسة الحقوق الوطنية والمدنية والعائلية،[4]
3- تحديد الإقامة،[5]
4- المنع من الإقامة،[6]
5- المصادرة الجزئية للأموال،[7]
6- المنع المؤقت من ممارسة مهنة أو نشاط،[1]

---

[1] تنص م 5/323 ق ع ف على:
Les personnes physiques coupables des délits prévus au présent chapitre encourent également les peines complémentaires suivantes:
1° L'interdiction, pour une durée de cinq ans au plus, des droits civiques, civils et de famille, suivant les modalités de l'article 131-26;
2° L'interdiction, pour une durée de cinq ans au plus, d'exercer une fonction publique ou d'exercer l'activité professionnelle ou sociale dans l'exercice de laquelle ou à l'occasion de laquelle l'infraction a été commise;
3° La confiscation de la chose qui a servi ou était destinée a commettre l'infraction ou de la chose qui en est le produit, à l'exception des objets susceptibles de restitution;
4° La fermeture, pour une durée de cinq ans au plus, des établissements ou de l'un ou de plusieurs des établissements de l'entreprise ayant servi à commettre les faits incriminés;
5° L'exclusion, pour une durée de cinq ans au plus, des marchés publics;
6° L'interdiction, pour une durée de cinq ans au plus, d'émettre des chèques autres que ceux qui permettent le retrait de fonds par le tireur auprès du tiré ou ceux qui sont certifiés;
7° L'affichage ou la diffusion de la décision prononcée dans les conditions prévues par l'article 131-35

[2] القانون رقم 23/06 المؤرخ في 2006/12/20. ج ر87.

[3] تنص م9 مكرر/1 ق ع على: "في حالة الحكم بعقوبة جنائية تأمر المحكمة وجوبا بالحجر القانوني الذي يتمثل في حرمان المحكوم عليه من ممارسة حقوقه المالية أثناء تنفيذ العقوبة الأصلية".

[4] حسب م9 مكرر1 يتمثل الحرمان من ممارسة الحقوق الوطنية والمدنية والعائلية في: 1- العزل أو الإقصاء من جميع الوظائف والمناصب العمومية التي لها علاقة بالجريمة، 2- الحرمان من حق الانتخاب أو الترشح ومن حمل أي وسام، 3- عدم الأهلية لأن يكون مساعدا محلفا أو خبيرا أو شاهدا على أي عقد أو شاهدا أمام القضاء إلا على سبيل الاستدلال، 4- الحرمان من الحق في حمل الأسلحة وفي التدريس وفي إدارة مدرسة أو الخدمة في مؤسسة للتعليم بوصفه أستاذا أو مدرسا أو مراقبا، 5- عدم الأهلية لأن يكون وصيا أو قيما، 6- سقوط حقوق الولاية أو بعضها...".

[5] وهو حسب نص م11 ق ع إلزام المحكوم عليه بأن يقيم في نطاق إقليمي يعينه الحكم لمدة لا تتجاوز خمس سنوات.

[6] حسب نص م12 ق ع فإن المنع من الإقامة هو حظر تواجد المحكوم عليه في بعض الأماكن، ولا يجوز أن تفوق مدته في مواد الجنح خمس سنوات ما لم ينص القانون على خلاف ذلك...

[7] المصادرة حسب م15 ق ع هي الأيلولة النهائية إلى الدولة لمال أو مجموعة أموال معينة، أو ما يعادل قيمتها عند الاقتضاء.

7- إغلاق المؤسسة،[2]

8- الإقصاء من الصفقات العمومية،[3]

9- الحظر من إصدار الشيكات، و/أو استعمال بطاقات الدفع،[4]

10- تعليق أو سحب رخصة السياقة أو إلغاؤها مع المنع من استصدار رخصة جديدة،[5]

11- سحب جواز السفر،[6]

12- نشر أو تعليق حكم أو قرار الإدانة.[7]

وعليه نرى أنه من الأجدر أن تحيل م394مكرر6 تطبيق العقوبات التكميلية إلى نص م9 ق ع.

الفرع الرابع: المبادئ المشتركة بين جرائم الاعتداء على أنظمة المعالجة الآلية للمعطيات.

تتلخص هذه المبادئ فيما يلي:

أولا: مبدأ مسؤولية الشخص المعنوي.

نص على ذلك المشرع الفرنسي في م 6/323 ق ع ف وفقا للشروط التي نصت عليها م2/121 ق ع ف.[1]

---

[1] وحسب نص م16 مكرر ق ع يجوز الحكم على الشخص المدان لارتكابه جناية أو جنحة بالمنع من ممارسة مهنة أو نشاط، في حال ثبت للجهة القضائية أن ثمة صلة مباشرة للجريمة بممارسة المهنة أو النشاط، وأن هناك خطر في استمرار ممارسته لأي منهما، ولا يجوز أن يتجاوز المنع بالنسبة للجنح مدة خمس سنين.

[2] وحسب نص م16 مكرر1 ق ع يترتب على عقوبة غلق المؤسسة منع المحكوم عليه من أن يمارس فيها النشاط الذي ارتكبت الجريمة بمناسبته، ويحكم بهذه العقوبة لمدة لا تزيد عن خمس سنوات في حالة الإدانة بارتكاب جنحة.

[3] وحسب نص م16 مكرر2 ق ع يترتب على هذه العقوبة منع المحكوم عليه من الممارسة بصفة مباشرة أو غير مباشرة في أية صفقة عمومية لمدة لا تزيد عن خمس سنوات في حالة الإدانة بارتكاب جنحة.

[4] وحسب نص م16 مكرر3 ق ع يترتب على هذه العقوبة إلزام المحكوم عليه بإرجاع الدفاتر والبطاقات التي بحوزته أو التي عند وكلائه إلى المؤسسة المصرفية المصدرة لها، لمدة لا تتجاوز خمس سنوات في حالة الإدانة لارتكاب جنحة. ولا يطبق هذا الحظر على الشيكات التي تسمح بسحب الأموال من طرف الساحب لدى المسحوب عليه أو تلك المضمنة.

[5] وحسب نص م16 مكرر4 ق ع فإن مدة التعليق أو السحب لا تزيد عن خمس سنوات من تاريخ صدور الحكم بالإدانة.

[6] وحسب نص م16 مكرر5 ق ع فإن مدة السحب لا تزيد عن خمس سنوات في حالة الإدانة من أجل جناية أو جنحة.

[7] حسب نص م18 ق ع يجوز للمحكمة عند الحكم بالإدانة أن تأمر في الحالات التي يحددها القانون بنشر الحكم بأكمله أو مستخرج منه في جريدة أو أكثر يعينها، أو بتعليقه في الأماكن التي يبينها، وذلك كله على نفقة المحكوم عليه، على ألا تتجاوز مصاريف النشر المبلغ الذي يحدده الحكم بالإدانة لهذا الغرض، وألا تتجاوز مدة التعليق شهرا واحدا.

يسأل الشخص المعنوي عن هذه الجرائم سواء بصفته فاعلا أصليا أو شريكا أو متدخلا، كما يسأل عن الجريمة التامة أو عن الشروع فيها،[2] كل ذلك بشرط أن تكون الجريمة قد ارتكبت لحساب الشخص المعنوي، بواسطة أحد أعضائه أو ممثليه (م2/121 ق ع ف). ولا تستبعد مسؤولية الشخص المعنوي الجزائية المسؤولية الجزائية للأشخاص الطبيعية (م2/121 فقرة 3 ق ع ف).

والعقوبات التي تطبق على الشخص المعنوي في القانون الفرنسي هي الغرامة ومقدارها خمسة أمثال الغرامة التي يحكم بها على الشخص الطبيعي كحد أقصى، والعقوبات المنصوص عليها في م39/131 ق ع ف وهي: الحل، الحرمان من النشاط، الرقابة القضائية، غلق المنشأة، الاستبعاد من التعامل في الأسواق العامة، الحرمان من الاكتتاب العام في الادخار، الحرمان المنصوص عليه في م39/131 رقم 2 والمتعلق بالحرمان من النشاط الذي بسببه أو بمناسبته ارتكبت الجريمة، سواء كان الحرمان مؤبدا أو لمدة لا تتجاوز خمس سنوات.[3]

أما المشرع الجزائري فقد نص في م394 مكرر4 على مسؤولية الشخص المعنوي بالنسبة لهذه الجرائم، وشدد العقوبة عليه حيث تبلغ خمس مرات الحد الأقصى للغرامة المقررة بالنسبة للشخص الطبيعي، وبناء عليه، فإن أقصى عقوبة أصلية يجوز أن يعاقب بها الشخص المعنوي هي 25 مليون دينار (م394 مكرر2 ق ع).

ثانيا: مبدأ المعاقبة على الشروع.

لا يتم العقاب في الشروع إلا في الجنايات لخطورتها، وفي الجنح إذا وجد نص خاص يقضي بذلك، ولا يعاقب على الشروع في المخالفات إطلاقا.

ونظرا لخطورة جرائم المعالجة الآلية لمعطيات الكمبيوتر، فقد نصت م394 مكرر7

---

[1] Article 323-6-1 "Les personnes morales peuvent être déclarées responsables pénalement, dans les conditions prévues par l'article 121-2, des infractions définies au présent chapitre".

[2] علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب الآلي، دار الجامعة الجديدة، الأزاريطة، الإسكندرية، مصر 2010، ص115.

[3] Article 323-6-2 "Les peines encourues par les personnes morales sont:
1° L'amende, suivant les modalités prévues par l'article 131-38;
2° Les peines mentionnées à l'article 131-39.
L'interdiction mentionnée au 2° de l'article 131-39 porte sur l'activité dans l'exercice ou à l'occasion de l'exercice de laquelle l'infraction a été commise".

ق ع على العقاب في الشروع بالعقوبات ذاتها المقررة للجرائم محل الدراسة إذا وقعت تامة، وهو ما نصت عليه م7/323 ق ع ف.[1]

والملاحظ بالنسبة للشروع أو المحاولة أن المشرع الجزائري في م394 مكرر/1 ق ع قد نص على الشروع استقلالا بالنسبة لجريمة الدخول أو البقاء غير المشروع، حيث جاء في نص المادة: "يعاقب ...كل من يدخل أو يبقى...أو **يحاول ذلك**"، ثم نص بعد ذلك على الشروع بالنسبة لكل الجنح المنصوص عليها في القسم، وهو مسلك منتقد، فما دام المشرع قد نص على الشروع بالنسبة لكل الجنح الواردة في القسم المتعلق بالمساس بأنظمة المعالجة الآلية للمعطيات، فما الداعي للنص عليه أيضا في م394 مكرر/1 ق ع؟

ثالثا: مبدأ المعاقبة على الأعمال التحضيرية المادية الجماعية.

وهو ما يعرف أيضا بالاتفاق الجزائي، والعقاب على هذا الاتفاق خروج على القواعد العامة، وهو محل خلاف فقهي، إذ أن القواعد العامة تقضي بأن العقاب لا يتقرر إلا بالنسبة للجرائم التامة أو التي تقف عند حد الشروع أو المحاولة،[2] لذلك يرى جانب من الفقه أنه لا يوجد شروع في الاتفاق الجزائي، وله حججه، ومنها أن الاتفاق حالة نفسية تتم بتلاقي الإرادات، ولا يقع إلا كاملا ولا يتصور فيه بدء في التنفيذ، يضاف إلى ذلك أن المشرع المصري لا يعتبر الدعوة إلى الاتفاق شروعا، ولكن جريمة قائمة بذاتها، معاقب عليها بنص م 97 ق ع م،[3] ولكن جانبا آخر من الفقه يرى غير ذلك، فإذا توافر القصد الجنائي ولم يتم الاتفاق لأسباب لا دخل لإرادة الجاني فيها فالعقاب على الشروع متعين، إذا كان الاتفاق جناية، أو جنحة بوجود نص خاص.[4]

الملاحظ أن المشرع الجزائري في م394 مكرر5 قد عاقب على الاتفاق من أجل إعداد جريمة أو أكثر من الجرائم محل الدراسة، باعتبارها مرحلة من مراحل الجريمة تسبق الشروع، وبقراءة نص م394 مكرر7 سالفة الذكر نجد أن المشرع قد جرم الشروع بالنسبة لجميع جرائم المعطيات بما فيها جريمة الاتفاق، وهذا المسلك منتقد عند جانب من الفقه، حيث أن تجريم الاتفاق الجنائي في

---

[1] Article 323-7.
"La tentative des délits prévus par les articles 323-1 à 323-3 est punie des mêmes peines".

[2] علي عبد القادر القهوجي، المرجع السابق، ص117.

[3] محمد خليفة، المرجع السابق، ص118.

[4] المرجع نفسه، ص118.

حد ذاته منتقد عندهم، وقد حكم بعدم دستوريته في مصر، لأنه يعاقب على مجرد العزم، فكيف بالعقاب على مجرد الشروع في هذا الاتفاق؟ فالمشرع هنا يقوم بالتجريم على وجود إرادة لم تلتق مع إرادات أخرى، لأنها لو التقت لكان الاتفاق مكتملا، وكأن المشرع يجرم مجرد النوايا.[1]

بناء على ما تقدم يحسن بالمشرع الجزائري أن يحذو حذو نظيره الفرنسي، في إخراجه لجريمة الاتفاق الجنائي من نظام الشروع، حيث نص المشرع الفرنسي على هذه الجريمة في م4/323 ق ع ف، أما العقاب على الشروع فقصره على الجرائم الواردة في المواد: 323-1 إلى 323-3 ق ع ف، حسب نص م323-7 ق ع ف.

المشرع الفرنسي في م4/323 ق ع ف،[2] قد عاقب على مساهمة أكثر من شخص في ارتكاب أفعال مادية تحضيرية تهدف إلى ارتكاب إحدى جرائم الاعتداء على نظم المعالجة الآلية للمعطيات، وهو الاتجاه نفسه الذي تبناه المشرع الجزائري، والغرض من هذا النص هو تقرير نوع من الحماية المتقدمة والوقائية لنظم المعالجة الآلية للمعطيات، ضد المخاطر الناشئة عن النشاط غير المشروع لبعض نوادي المعلوماتية، أو قراصنة المعلوماتية.[3]

ويشترط لتطبيق نص هذه المادة أن يكون هنالك اتفاق بين شخصين على الأقل، بهدف التحضير لارتكاب إحدى الجرائم سالفة الذكر، وأن يتخذ هذا التحضير صورة فعل أو أفعال مادية صادرة عن أعضاء الاتفاق،[4] ومن أمثلتها تبادل المعلومات اللازمة لتنفيذ الجريمة، كالكشف عن الرقم السري أو الكودي، أو كلمة السر للدخول إلى النظام، أو كيفية تجاوزها، أو استخدام قنبلة زمنية أو فيروس ...ويدخل ضمن هذه الأعمال المادية حضور شخص لاجتماع تناقش فيه مثل تلك الأفعال.[5]

---

[1] المرجع نفسه، ص119.

[2] Article 323-4.
"La participation à un groupement formé ou à une entente établie en vue de la préparation, caractérisée par un ou plusieurs faits matériels, d'une ou de plusieurs des infractions prévues par les articles 323-1 à 323-3 est punie des peines prévues pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée".

[3] علي عبد القادر القهوجي، المرجع السابق، ص117.

[4] المرجع نفسه، ص117.

[5] المرجع نفسه، ص118.

ويجب لتطبيق نص المادة، أن يكون نشاط الجماعة موجها نحو هدف محدد هو التحضير لارتكاب جريمة من جرائم الاعتداء على نظم المعالجة الآلية للمعطيات، فلا يعاقب استنادا إلى هذا النص إذا كان الهدف ارتكاب جريمة أخرى كجريمة تقليد البرنامج المنصوص عليها في قانون حماية المؤلف.[1]

ويجب توافر القصد الجنائي لدى أعضاء الجماعة والمتمثل في توافر العلم لكل واحد منهم أنه عضو في جماعة إجرامية، وأن تتجه إرادة كل واحد منهم إلى تحقيق نشاط إجرامي معين، وهو العمل التحضيري، ولا يشترط أن يكون كل واحد منهم عالما بنشاط الآخر.[2]

ويعاقب المشرع الفرنسي على هذا النشاط الإجرامي بعقوبة الجريمة التي يتم التحضير لها إذا وقعت تامة، فإذا تعددت الجرائم التي يتم التحضير لها تكون العقوبة هي عقوبة الجريمة الأشد حسب القواعد العامة.

إذا ساهم أعضاء الاتفاق في الجريمة التي تم التحضير لها، نكون أمام تعدد مادي للجرائم، إذ أن الجريمة الأولى مستقلة عن الجريمة الثانية، وإذا وجدت علاقة سببية بين الأعمال التحضيرية التي قاموا بها وبين الجريمة الثانية التي وقعت، فإنهم يعتبرون في الوقت نفسه مساهمين في تلك الجريمة باعتبارهم فاعلين أو شركاء أو متدخلين حسب الأحوال.[3]

[1] المرجع نفسه، ص118.

[2] علي عبد القادر القهوجي، المرجع السابق، ص118.

[3] المرجع نفسه، ص119.

المطلب الثاني: جريمة الدخول أو البقاء غير المشروع في نظام المعالجة الآلية للمعطيات.

تجرم م323-1 ق ع ف وتعاقب على فعل الدخول أو البقاء غير المشروعين في نظام المعالجة الآلية للبيانات (المعطيات) أو في جزء منه، وتشدد العقوبة إذا نتج عن هذا الدخول أو البقاء محو أو تغيير في البيانات الموجودة في النظام، أو حدث تعييب لتشغيل ذلك النظام، وقد تطرقت لهذه الجريمة م394مكرر ق ع، وهي مأخوذة عن م323-1 ق ع ف.[1]

تتمثل الصورة البسيطة لهذه الجريمة في مجرد الدخول أو البقاء غير المشروع، بينما تتحقق الصورة المشددة بتحقق الظرف المشدد لها، والملاحظ أن المشرع الفرنسي قد نص على ظرفين مشددين لهذه الجريمة، وكذلك فعل المشرع الجزائري.

نصت الاتفاقية العربية لمكافحة تقنية المعلومات سالفة الذكر في م6 على ضرورة تجريم الدخول أو البقاء، وكل اتصال غير مشروع مع كل أو جزء من تقنية المعلومات أو الاستمرار بهذا الاتصال، واقترحت ظرفين مشددين للجريمة تشدد على إثرهما العقوبة، وذلك إذا نتج عن الدخول أو البقاء غير المشروعين محو أو تعديل أو تشويه أو نسخ أو نقل أو تدمير للبيانات المحفوظة وللأجهزة والأنظمة الإلكترونية وشبكات الاتصال، وإلحاق الضرر بالمستخدمين والمستفيدين، أو إذا تعلق الأمر بالحصول على معلومات حكومية سرية.

[1] تنص م323-1 ق ع ف على ما يلي :

Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 30 000 euros d'amende.

Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de trois ans d'emprisonnement et de 45 000 euros d'amende.

Lorsque les infractions prévues aux deux premiers alinéas ont été commises à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'Etat, la peine est portée à cinq ans d'emprisonnement et à 75 000 € d'amende.

الفرع الأول: جريمة الدخول أو البقاء البسيطة.

بينت أركانَ هذه الجريمة وعقوبتها م323-1/1ق ع ف، وم394مكرر ق ع، وتتكون هذه الجريمة إضافة إلى الركن الشرعي المتمثل في نصوص التجريم المذكورة في المادتين أعلاه، من ركن مادي، وآخر معنوي.

أولا: الركن المادي لجريمة الدخول أو البقاء البسيطة.

يتكون الركن المادي في هذه الجريمة من نشاط إجرامي، يتمثل إما في فعل الدخول (الولوج) غير المشروع (غير المرخص به) إلى نظام المعالجة الآلية للمعطيات كله أو جزء منه، وإما في فعل البقاء غير المشروع في هذا النظام أو في جزء منه.[1]

1- مفهوم الدخول غير المشروع إلى النظام.

يرى الفقه الفرنسي –بحق– أن للدخول أو الولوج معنى ماديا، وآخر معنويا[2]، ولا يقصد بالدخول المعنى المادي كالدخول إلى منزل أو حديقة، وإنما القصد المعنى المعنوي، الذي يشبه الدخول إلى فكرة أو ملكة التفكير لدى الإنسان، وهو يفترض إقامة اتصال مع النظام المعلوماتي من قبل شخص غير مرخص له بذلك،[3] ووفقا لهذا المعنى الأخير فإن الولوج إلى النظام المعلوماتي يتحقق بأية صورة من صور التعدي، بطريقة مباشرة أو غير مباشرة،[4] من ذلك استعمال كلمة السر الخاصة بشخص مسموح له بالدخول، حتى لو كان بعلمه طالما أنه لا يملك حق منح ترخيص الدخول، أو استعمال نمط اتصال غير مرخص به، لعدم احترامه شروط الاتصال، أو استعمال برنامج متطور يسمح بالدخول إلى النظام كاستعمال برنامج "حصان طروادة"،[5] فلا تهم الوسيلة التي تسمح بالدخول غير الشرعي إلى النظام، إذ يمكن الدخول عن طريق كلمة السر الحقيقية إذا لم يكن للجاني حق استخدامها، أو باستخدام برنامج أو شفرة خاصة،[6] أو عن طريق استخدام الرقم الكودي

---

[1] علي عبد القادر القهوجي، المرجع السابق، ص120.

[2] لذلك استعمل المشرع الفرنسي مصطلح "accès" بدلا من "entrée" لأنه أكثر ملاءمة في هذا المجال. محمد خليفة، المرجع السابق، ص141.

[3] Béatrice Clément et autres, op cit, p266.

[4] بيومي حجازي، المرجع السابق، ص28.

[5] Béatrice Clément et autres, op cit, p266.

[6] عبد الحليم رمضان، المرجع السابق، ص51.

لشخص آخر، أو الدخول من خلال شخص مسموح له بالدخول، أو عن طريق التوصل للرقم الكودي للدخول، أو عن طريق تجاوز نظام الحماية في حالة وجود هذا النظام، وسواء تم الدخول عن بعد عن طريق شبكات الاتصال، أو لطرفيات سواء كانت محلية أو عالمية.[1]

وحسب القضاء فإنه لا يشترط لقيام الجريمة تمتع النظام المعلوماتي بحماية فنية، في الوقت الذي يصبح فيه الولوج ممنوعا عن الجمهور، أي غير مفتوح لهم، ومحصورا على فئة من الأشخاص(l'accès n'est pas public, mais restreint à certaines personnes)، وعليه لا يمكن تصور أبدا دخولا غير مشروع إلى النظام المعلوماتي المفتوح للجمهور من مثل مواقع الانترنت،[2] حتى ولو تم ذلك دون الحصول على اشتراك تقديم خدمات تلك الشبكة، ويمتد الدخول ليسري على صندوق البريد الإلكتروني المتواجد بالجهاز،[3] وقد قررت محكمة استئناف باريس في أحد أحكامها بأنه "في غياب وضع حماية للبرنامج أو تعبير صريح لإرادة مسيري المؤسسة بحظر الولوج إلى النظام على الجمهور، فإن الجنحة لا تقوم"،[4] فلا تقوم الجريمة إذا لم يكن صاحب النظام قد عبر عن رغبته في عدم السماح للآخرين بالدخول.[5]

ويعد الدخول أو الولوج ذاته جريمة وقتية، تقع من أي شخص، حيث يستوي أن يكون من الخبراء أو حتى من الأفراد العاديين، وسواء كان الدخول للقيام بعمل غير مشروع، أو لمجرد الفضول وحب الاستطلاع،[6] وسواء كان يستطيع أن يستفيد من الدخول أم لا، حيث يكفي أن يكون الجاني ممن ليس لهم الحق في الدخول، أو من الذين ليس لهم الحق في الدخول بالطريقة التي دخلوا بها، وعليه فإن الجريمة تقوم في كل حالة يكون فيها الدخول مخالفا لشروط الدخول المنصوص عليها قانونا، أو المنصوص عليها اتفاقا، أو ضد إرادة من له حق السيطرة على النظام، كأن يكون الدخول يتطلب إلزاما دفع مبلغ من النقود، وتم الدخول دون دفع المبلغ.[7]

---

[1] عبد القادر القهوجي، المرجع السابق، ص121.

[2] Béatrice Clément et autres, op cit, p 266.

[3] غنام محمد غنام، المرجع السابق، ص130.

[4] Béatrice Clément et autres, op cit, p 266.

[5] غنام محمد غنام، المرجع السابق، ص130.

[6] مدحت عبد الحليم رمضان، المرجع السابق، ص51.

[7] علي عبد القادر القهوجي، المرجع السابق، ص121.

وتتم الجريمة سواء أتم الدخول إلى النظام كله أو إلى جزء منه فقط، وتتوافر الجريمة في حالة الجاني الذي يسمح له بالدخول إلى جزء من النظام، فيستغل الفرصة، ويدخل إلى جزء آخر غير مسموح له بالدخول إليه، بشرط أن يكون العنصر الذي تم الدخول إليه يدخل في برنامج متكامل قابل للتشغيل، فلا تتوافر الجريمة إذا تم الدخول إلى عنصر لا علاقة له بنظام المعالجة الآلية للمعطيات، مثل الدخول إلى البرنامج منعزلا عن غيره من العناصر، ولا تتوافر الجريمة أيضا في الحالة التي يقتصر فيها الشخص على مجرد قراءة الشاشة.[1]

وتقوم الجريمة بفعل الدخول إلى النظام، بغض النظر عن أي نتيجة أخرى، فلا يشترط لقيامها التقاط الجاني للمعلومات التي يحتويها النظام أو بعضها، أو استعمالها، بل تقوم الجريمة حتى ولو لم تكن للجاني المقدرة الفنية على تنفيذ العمليات على النظام، فالعبرة في هذه الجريمة هي بتحقق السلوك الإجرامي بغض النظر عن النتيجة الإجرامية، فالركن المادي لهذه الجريمة يتكون من السلوك الإجرامي فقط،[2] ولا يتطلب علاقة سببية، فجريمة الدخول من جرائم الخطر لا الضرر.[3]

2- مفهوم البقاء غير المشروع داخل النظام.

الصورة الثانية لهذه الجريمة هي البقاء غير المشروع داخل النظام، أي التواجد داخل نظام المعالجة الآلية للمعطيات ضد إرادة من له الحق في السيطرة على هذا النظام، وقد يتحقق البقاء المعاقب عليه مستقلا عن الولوج داخل النظام، وقد يجتمعان معا، ويكون البقاء معاقبا عليه استقلالا حين يكون الولوج إلى النظام مشروعا، كمن يتحقق ولوجه بالصدفة أو عن طريق الخطأ، حيث يتوجب في هذه الحالة الانسحاب فورا من النظام، فإذا بقي رغم ذلك فإنه يعاقب على جريمة البقاء غير المشروع (غير المصرح به)، ويتحقق البقاء أيضا في الحالة التي يستمر فيها الجاني باقيا داخل النظام بعدد المدة المسموح له بها بالبقاء داخله، أو في الحالة التي يطبع فيها نسخة من المعلومات ولم يكن يسمح له إلا بالرؤية والاطلاع فقط[4]، ويتحقق ذلك أيضا بالنسبة للخدمات المفتوحة للجمهور كالخدمات الهاتفية، التي يستطيع الجاني فيها الحصول على الخدمة دون دفع المقابل، أو الحصول على الخدمة مدة أطول من المدة التي دفع مقابلها، عن طريق استخدام وسائل أو عمليات غير مشروعة،

---

[1] المرجع نفسه، ص122.

[2] المرجع نفسه، ص122.

[3] د. محمود أحمد طه، المواجهة التشريعية لجرائم الكمبيوتر والانترنت، دراسة مقارنة، دار الفكر والقانون، المنصورة، مصر 2013، ص26.

[4] علي عبد القادر القهوجي، المرجع السابق، ص122.

ومن أمثلة ذلك ما حكم به القضاء الفرنسي من أن استعمال العمال لجهاز المينيتال – ليلا ونهارا – الذي وضع تحت تصرفهم من قبل مستخدمهم، قصد ربح نقاط وهدايا، تقوم به هذه الجنحة.[1]

وقد يجتمع الدخول غير المشروع مع البقاء غير المشروع، عندما لا يكون للجاني الحق في الدخول إلى النظام، ويدخل إليه متعمدا، ثم يبقى داخل النظام بعد ذلك، ويتحقق هنا الاجتماع المادي بين الجريمتين.

والسؤال المطروح: متى تنتهي جريمة الدخول؟ ومتى تبدأ جريمة البقاء؟[2]

رأى جانب من الفقه أن جريمة الدخول تتحقق منذ اللحظة التي يتم الدخول فيها فعلا إلى البرنامج، ويفترض البقاء لفترة قصيرة من الزمن تنتهي عندها جريمة الدخول وتكتمل، وبعدها تبدأ جريمة البقاء داخل النظام وتنتهي بانتهاء حالة البقاء.

ويعاب على هذا الرأي عدم تحديده لحظة بداية جريمة البقاء بطريقة قاطعة، مما حذا بجانب آخر من الفقه إلى تحديد تلك اللحظة منذ الوقت الذي يعلم فيه الداخل أن بقاءه داخل النظام غير مشروع، وانتقد هذا الرأي أيضا من جانب صعوبة إثبات علم الداخل، مما جعل جانبا ثالثا من الفقه يرى أن جريمة البقاء تبدأ من اللحظة التي ينذر فيها المتدخل بأن تواجده غير مشروع أو أصبح غير مشروع، ولكن يعاب على هذا الرأي أيضا رغم وجاهته، افتراض وجود جهاز إنذار يقوم بهذه المهمة،[3] وهو ما يدفع إلى القول بافتراض الحماية الأمنية المسبقة لقيام الجريمة، وهو ما لم يتطلبه المشرع.

ولذلك فإن جانبا من الفقه يرى أن جريمة البقاء تبدأ من اللحظة التي يبدأ فيها الداخل التجول داخل النظام، أو يستمر في التجول داخله بعد انتهاء الوقت المحدد، لأن الفرضية تتعلق بدخول غير مشروع، فالجاني يعلم أن دخوله غير مشروع، فإذا دخل وظل ساكنا تظل الجريمة جريمة دخول، أما إذا بدأ في التجول فإن جريمة البقاء داخل النظام تبدأ منذ تلك اللحظة.[4]

---

[1] Béatrice Clément et autres, op cit, p267.

[2] القهوجي، المرجع السابق، ص123.

[3] القهوجي، المرجع السابق، ص123.

[4] المرجع نفسه، ص124.

وعلى كل فإن المشكلة من الناحية العملية لا تثار، إذ أن المشرع عاقب في النص نفسه على الدخول أو البقاء بالعقوبة ذاتها.

ويرى البعض بأن المشرع جرم البقاء غير المشروع داخل النظام لمن كان دخوله إلى النظام بطريق الصدفة وانتفى لديه القصد الجنائي، أي قصد الدخول غير المشروع، ورغم ذلك بقي في النظام واتجهت إرادته إلى ذلك.[1]

ويكفي لتحقق جريمة البقاء غير المشروع داخل النظام، أن يكون البقاء داخل النظام كله، أو في جزء منه، ولا يشترط وقوع أي شكل من أشكال الضرر.[2]

وهذه الجريمة، أي جريمة الدخول غير المشروع إلى نظام المعالجة الآلية للمعطيات، أو البقاء غير المشروع فيها، جريمة سلوك مجرد، تقع وتكتمل بمجرد الانتهاء من السلوك المكون لها وهو الدخول أو البقاء غير المشروعين.[3]

ثانيا: الركن المعنوي لجريمة الدخول أو البقاء البسيطة.

جريمة الدخول أو البقاء غير المشروع جريمة عمدية، يتخذ الركن المعنوي فيها صورة القصد الجنائي، بنص م394 مكرر ق ع "...عن طريق الغش.."، وكذلك بنص م323-1 ق ع ف والتي ذكرت لفظ الغش صراحة "Frauduleusement"، ولعل الحكمة من جعل هذه الجريمة عمدية هي رغبة المشرع في الموازنة بين حماية خصوصية الأنظمة المعلوماتية، وحماية حرية الأفراد في استخدام الانترنت.[4]

يتطلب القصد الجنائي العلم والإرادة، حيث يجب لقيام هذه الجريمة، أن يعلم الجاني بأن ليس له الحق بالدخول إلى النظام أو البقاء فيه، ورغم ذلك تتجه إرادته إلى هذا الفعل غير المشروع.

وعليه لا يتوافر الركن المعنوي إذا كان دخول الشخص أو بقاؤه داخل النظام مسموح به، كما لا يتوافر هذا الركن وبالتالي لا تقوم الجريمة إذا وقع الشخص في خطأ في الواقع سواء أتعلق بمبدإ

---

[1] أمين أعزان، المرجع السابق، ص102.

[2] القهوجي، المرجع السابق، ص124.

[3] عبد القادر القهوجي، ص125.

[4] محمد خليفة، المرجع السابق، ص163.

الحق في الدخول أو في البقاء، أو في نطاق هذا الحق، كأن يجهل وجود حظر للدخول أو البقاء، أو كان يعتقد خطأ أنه مسموح له بالدخول أو البقاء،[1] وفي هذا الشأن يجوز إجراء مقاربة بين هذه الجريمة وجريمة انتهاك حرمة منزل المنصوص عليها في م226-4 من ق ع ف.[2]

ولا يبدو من خلال نصوص التجريم السابقة أنها تتطلب قصدا خاصا،[3] رغم ذلك يرى جانب من الفقه الفرنسي أن لفظ الغش يحمل في طياته قصدا خاصا، هو حصول الغش، ويعرفون الغش على ضوء ما عرفه الفقه في جريمة السرقة: "أخذ مال الغير، ونقل الحيازة بدون رضا المالك"، ثم يسقطونه على جريمة الدخول أو البقاء ليتوصلوا بأن الغش يكون عند معرفة الشخص بغياب حق الدخول أو البقاء في الأنظمة.[4]

غير أن معرفة الجاني بأن ليس له الحق في الدخول أو البقاء فيه لا يشكل قصدا خاصا، بل هو من متطلبات قيام القصد العام، فالقصد الخاص عبارة عن علم وإرادة ينصرفان إلى وقائع لا تدخل ضمن عناصر الجريمة، كما أن استعمال لفظ الغش، لا يدل إلا على معنى واحد وهو أن الجريمة عمدية لا أكثر، يكفي لقيام ركنها المعنوي توافر القصد العام.[5]

ولا عبرة بالباعث، إذ تقوم الجريمة مهما كان الباعث أو الدافع لها، حتى ولو كان مجرد فضول، أو تنزه، أو إثبات القدرة على الانتصار على النظام.[6]

---

[1] عبد القادر القهوجي، المرجع السابق، ص126.

[2] Béatrice Clément et autres, op cit, p267.

[3] في بعض الجرائم تصبح النية الخاصة أو الباعث عنصرا ثالثا داخلا في القصد الجنائي، يضاف إلى عنصري الإرادة والعلم، فيوصف القصد الجنائي حينئذ بأنه قصد جنائي خاص تمييزا له عن القصد العام. يراجع: د. إبراهيم الشباصي، الوجيز في شرح قانون العقوبات الجزائري، القسم العام، دار الكتاب اللبناني، بيروت، لبنان (دون ذكر سنة النشر)، ص89. وأيضا: د. علي عبد القادر القهوجي، شرح قانون العقوبات القسم العام، النظرية العامة للجريمة، (دون ذكر دار النشر) 2002، ص381، وأيضا: إبراهيم بلعيات، أركان الجريمة وطرق إثباتها في قانون العقوبات الجزائري، دار الخلدونية، الجزائر 2007، ص123.

[4] محمد خليفة، المرجع السابق، ص168.

[5] المرجع نفسه، ص168.

[6] عبد القادر القهوجي، الحماية الجنائية... المرجع السابق، ص126.

الفرع الثاني: جريمة الدخول أو البقاء المشددة.

نصت م394 مكرر/2، 3 ق ع، على ظرف مشدد، تشدد بسببه عقوبة جريمة الدخول أو البقاء داخل النظام، حينما ينتج عن الدخول أو البقاء حذف أو تغيير لمعطيات المنظومة، أو تخريب نظام اشتغال المنظومة، و الأمر نفسه ذكرته م323-1 فقرة 2 ق ع ف التي شددت العقوبة المترتبة عن الدخول أو البقاء إذا نتج عنها محو أو تعديل المعطيات التي يحتويها النظام، أو عدم صلاحية النظام لأداء وظائفه.

ويتحقق الظرف المشدد بوجود العلاقة السببية بين الدخول أو البقاء غير المشروعين والنتيجة الضارة التي لا يشترط فيها أن تكون مقصودة، لأن المشرع جرم الاعتداء المقصود على النظام باعتباره جريمة مستقلة عن هذه الجريمة، كما لا يشترط أن تكون النتيجة غير مقصودة، أي على سبيل الخطأ غير العمدي الذي قد يتخذ صورة الإهمال أو عدم الاحتراز أو الرعونة. فالظرف المشدد هنا ظرف مادي، حسب جانب من الفقه،[1] لكن جانبا آخر من الفقه يرى غير ذلك، إذ يرى أن النظر في الركن المعنوي أمر ضروري، فإن قصد الجاني النتيجة اعتبر ذلك مكونا لجريمة أخرى هي التلاعب بالمعطيات، وإن لم يقصدها أي كانت النتيجة عن طريق الخطأ قام الظرف المشدد، أي أن هذا الأخير لا يقوم إلا إذا لم يكن القصد عمديا، أي عن طريق الخطأ.[2]

ولا تقوم الجريمة في صورتها المشددة إذا كانت النتيجة الضارة ترجع إلى القوة القاهرة أو الحادث المفاجئ.[3]

وأوجد المشرع الفرنسي في م323-1/3 ظرفا أكثر تشديدا يتعلق بارتكاب الجرائم المنصوص عليها ضد نظام معلوماتي ذي طابع شخصي موضوع من قبل الدولة، ولم يبين النص، هل مجرد الدخول إلى هذا النظام يستوجب تشديد العقوبة؟ أم ضرورة توافر النتيجة الضارة؟ وهي محو أو تعديل المعطيات التي يحويها النظام، أو عدم صلاحية هذا الأخير لأداء وظائفه، والظاهر أن المشرع

[1] عبد القادر القهوجي، المرجع السابق، ص127.

[2] محمد خليفة، المرجع السابق، ص170.

[3] بيومي حجازي، المرجع السابق، ص37.

الفرنسي يشدد العقوبة بغض النظر عن النتيجة، إذ يرفع عقوبة السجن إلى خمس سنين، والغرامة إلى 75.000 يورو.

إذا توافرت جريمة الدخول أو البقاء غير المشروعين، سواء في صورتها البسيطة أو المشددة، استحق مرتكبها العقوبة المقررة لها.

يعاقب المشرع الفرنسي بعقوبة الحبس لمدة سنتين وبالغرامة المقدرة ب: 30.000 يورو، أما المشرع الجزائري فيعاقب على الصورة البسيطة لهذه الجريمة، بعقوبة الحبس وبعقوبة الغرامة، ويحكم بهاتين العقوبتين معا، أما عقوبة الصورة المشددة فهي ضعف عقوبة الصورة البسيطة، وعليه، وحسب م394مكرر ق ع فإن عقوبة الدخول أو البقاء في الصورة البسيطة هي الحبس من ثلاثة أشهر إلى سنة والغرامة من 50.000 دج إلى 100.000 دج، تضاعف العقوبة إذا ترتب عن الدخول أو البقاء حذف أو تغيير لمعطيات المنظومة (394مكرر/2 ق ع)، وهذا ظرف مشدد بسبب حدوث النتيجة الضارة وهي حذف أو تغيير معطيات المنظومة، وتكون العقوبة الحبس من ستة أشهر إلى سنتين والغرامة من 50.000دج إلى 150.000 دج إذا ترتب عن الدخول أو البقاء غير المشروعين تخريب نظام اشتغال المنظومة (م394مكرر/3 ق ع). وهنا فرق المشرع الجزائري في تشديد العقوبة بين حذف أو تغيير المعطيات، وتخريب نظام اشتغال المنظومة. والسؤال المطروح: لماذا هذا التمييز؟ خاصة وأن عقوبة م394 مكرر3/ ق ع ليست مغلظة بالمقارنة مع م 394 مكرر2، بل تكادان أن تتطابقا.

تضاعف العقوبات إذا استهدفت إحدى الجرائم المنصوص عليها الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام، دون الإخلال بتطبيق عقوبات أشد (م394 مكرر3 قانون العقوبات).

أما المشرع الفرنسي فقد جعل عقوبة الظرف المشدد الأول (حذف أو تغيير معطيات المنظومة أو تخريب اشتغالها) الحبس لمدة ثلاث سنوات، والغرامة بمقدار 45.000 يورو.

يعاقب الشخص المعنوي باعتباره فاعلا أو مساهما في الجريمة بالغرامة فقط، وهي خمس مرات الحد الأقصى للغرامة التي يحكم بها على الشخص الطبيعي، كما يعاقب على الشروع أو المحاولة بعقوبة الجريمة التامة، كما يعاقب على الأعمال التحضيرية المادية الجماعية بالعقوبات نفسها.

إن نظام التجارة الالكترونية هو نظام معلوماتي، يستند إلى أنظمة للمعالجة الآلية للمعطيات، شأنه في ذلك شأن أي نظام معلوماتي آخر، وهو بذلك معرض كغيره لأية مخاطر تهدد النظم المعلوماتية، لذا بات لزاما حماية مواقع التجارة الالكترونية سواء كانت وسيلتها الانترنت أو أية وسيلة إلكترونية أخرى، ولذلك فإن تجريم الدخول أو البقاء غير المشروعين في النظام المعلوماتي هو بمثابة الخط الدفاعي الأول لحماية نظم البيانات التي تخدم التجارة الإلكترونية، وكسب ثقة العملاء منتجين ومستهلكين.[1]

المطلب الثالث: إعاقة أو التسبب في تحريف تشغيل نظام معالجةمعطيات التجارة الالكترونية.

نصت على هذه الجريمة م2/323 ق ع ف،[2] وتتعلق بتجريم كل فعل من شأنه أن يؤدي إلى توقف تشغيل نظام المعالجة الآلية للمعطيات، أو جزء منه، منها على سبيل المثال، حذف أو تعديل أنماط المعالجة الآلية لنقل المعطيات، عن طريق القنابل المنطقية مثلا أو زرع فيروسات، أو إدخال برنامج تجسس، قد يدخله المستعمل نفسه دون أن يعرف ذلك عن طريق برنامج للألعاب الإلكترونية مثلا...[3]

ويجب لقيام هذه الجريمة توافر الركن المادي، والركن المعنوي.

[1] بيومي حجازي، المرجع السابق،ص ص38-39.

[2] Le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données est puni de cinq ans d'emprisonnement et de 75 000 euros d'amende.
Lorsque cette infraction a été commise à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'Etat, la peine est portée à sept ans d'emprisonnement et à 100 000 € d'amende.

[3] Jean larguier et autres, droit pénal spécial, 14ème édition, Dalloz, Paris 2008, p236.

الفرع الأول: الركن المادي.

استعمل المشرع الفرنسي لفظة إعاقة "entraver" ولفظة إفساد "fausser"، وهما لفظتان مرنتان تدلان على أن السلوك الإجرامي لهذه الجريمة ينصرف إلى كل فعل من شأنه إرباك عمل نظام معالجة المعطيات.

ويستوي أن يؤدي السلوك الإجرامي إعاقة نظام التشغيل أو الإرسال،[1] ويستوي أيضا أن يقع فعل الإعاقة (التعطيل) أو الإفساد على كل عناصر النظام، أو على إحداها فقط، سواء أكانت هذه العناصر مادية كجهاز الكمبيوتر ذاته أو شبكات الاتصال أو أجهزة النقل، أو معنوية كالبرامج والمعطيات.[2]

أولا: التعطيل أو الإعاقة.

لم يشترط المشرع الوسيلة التي تتم بها الإعاقة أو التعطيل (entrave)، فقد تكون الوسيلة مادية أو معنوية؛ حيث تكون الوسيلة مادية إذا وقعت على الأجهزة المادية للنظام، أو منعت الوصول إليها، كتخريبها، أو منع العاملين على الأنظمة من الوصول إلى المكان الذي توجد فيه، وتكون وسيلة الإعاقة معنوية إذا وقعت على المكونات المنطقية للنظام مثل البرامج والمعطيات عن طريق إدخال فيروسات مثلا، أو تعديل برنامج كلمة السر، أو جعل النظام يتباطأ في أدائه لوظائفه.[3]

ومن التطبيقات العملية لإعاقة "STAD"، زرع برامج الفيروسات، ومنها برنامج "حصان طروادة" التجسسي، وفيروس "I love you"، وإعطاء معلومات خاطئة لمنع عمل نظام الحماية الفني (T. Paris 1992)، تكثيف الرسائل للتأثير على ذاكرة الحاسب الآلي(T. Paris 1994).[4]

---

[1] عبد الحليم رمضان، المرجع السابق، ص54.

[2] علي عبد القادر القهوجي، المرجع السابق، ص128.

[3] علي عبد القادر القهوجي، المرجع السابق، ص129.

[4] Jean Larguier et autres, op cit, p240.

ويستوي أن تكون الإعاقة دائمة أو مؤقتة، فقد يتوقف النظام بشكل دائم، أو مؤقت أو بشكل متقطع على فترات كما في حالة إدخال قنبلة معلوماتية زمنية مبرمجة، كما يستوي أن يكون توقف النظام بالنسبة لجميع المستعملين، أو لأحدهم فقط.[1]

ويشترط في التوقف أو التعطيل أن يكون إيجابيا، أي أن يصدر عن الجاني نشاط إيجابي يؤدي إلى توقيف النظام، فلا يكفي مجرد امتناعه لقيام الجريمة، إلا إذا كان يقع على عاتقه واجب قانوني أو اتفاقي بتشغيل النظام، فامتنع عن التدخل بقصد تعطيله، فهنا تقوم الجريمة في حقه، لأن الامتناع هنا ليس امتناعا مجردا، وإنما هو امتناع مختلط بنشاط إيجابي يتمثل في رفض الجاني القيام بما يفرضه القانون أو الاتفاق عليه من واجب تشغيل النظام.[2]

ويكون التوقف مشروعا في حالة الإضراب إذا توافر سبب التبرير أو الإباحة وفقا لما ينص عليه القانون، فإذا لم تتوافر شروط سبب التبرير أو الإباحة أو حدث تجاوز لهذا السبب تطبق القواعد العامة بهذا الشأن.[3]

من الأمثلة العملية عن الإعاقة أو التعطيل قيام مجرمي المعلوماتية بتعطيل (STAD) عن طريق الإشباع (entrave du système par saturation)، ففي 2000/02/07 هوجمت العديد من المواقع على شبكة الانترنت عن طريق "إشباع الموقع"، وهو ما عرف بمصطلح "إنكار الخدمة"، بحيث أن تشبع الموقع نتيجة الكم الهائل من الرسائل الواردة عليه بحيث يصبح غير قادر على تقديم الخدمة لمتعامليه، ومست هذه الموجة مواقع معروفة مثل: yahoo، CNN.com Amazon.com وغيرها.

كما قد يكون التعطيل عن طريق ما يعرف ب: " Flaming " وهو عبارة عن هجمات من الانترنت هدفها تعطيل (STAD) عن طريق إحداث اكتظاظ كبير في ذاكرة الحاسب الآلي المهاجَم.[4]

---

[1] علي عبد القادر القهوجي، المرجع السابق، ص129.

[2] المرجع نفسه، ص129.

[3] عبد القادر القهوجي، المرجع السابق، ص130.

[4] Christiane Féral-SCHUHL, cyber droit, 6ème édition, Dalloz, Paris 2010, p918.

ثانيا: الإفساد أو التعييب.

الإفساد (التعييب) عبارة عن كل فعل يؤدي إلى جعل نظام المعالجة للمعطيات غير صالح للاستعمال السليم (وإن كان لا يؤدي إلى التعطيل)، بأن يعطي نتائج غير تلك التي كان من الواجب الحصول عليها.[1]

ووسائل الإفساد متعددة منها استخدام القنبلة المعلوماتية التي تجعل النظام غير صالح للاستعمال بإدخال معلومات تتكاثر داخله، أو استخدام برامج تحمل فيروسات مختلفة تجعل مخرجات النظام غير تلك التي كان من الواجب عليه أن يخرجها، بل إن الإفساد قد يتحقق عن طريق إتلاف العناصر المادية في النظام.[2]

يلاحظ أنه من الناحية العملية يصعب التمييز بين فعل الإفساد، وفعل الإعاقة، ويكفي النظر إلى مجرد الوسائل التي يتحقق بها كل فعل منهما.[3]

يلاحظ أيضا أن فعل الإعاقة أو الإفساد يشترك في جانب منه مع جريمة الإتلاف أو التخريب العادية، وبما أن النص على هذه الجريمة الأخيرة نص عام، ونص م2/323 ق ع نص خاص فإن فض التنازع الظاهري بين النصين يكون على أساس تغليب النص الخاص لأنه يتعلق بنظام المعالجة الآلية للمعطيات وليس بجميع الأشياء التي يمكن أن تقع عليها جريمة الإتلاف أو التخريب العادية.[4]

الفرع الثاني: الركن المعنوي.

جنحة إعاقة أو إفساد نظام المعالجة الآلية للمعطيات جريمة قصدية، يتخذ الركن المعنوي فيها صورة القصد الجنائي العام بعنصريه العلم والإرادة، حيث ينبغي لقيام هذا الركن أن تتجه إرادة الجاني إلى فعل الإعاقة أو فعل الإفساد أو هما معا، كما يجب أن يعلم أن نشاطه الإجرامي يؤدي إلى فعل التعطيل أو فعل الإفساد، وأن يعلم أن ذلك يتم دون رضا صاحب الحق أو ضد إرادته،[5] وهذا

[1] عبد القادر القهوجي، المرجع السابق، ص130.

[2] المرجع نفسه، ص130.

[3] عبد القادر القهوجي، المرجع السابق، ص130.

[4] المرجع نفسه، ص131.

[5] المرجع نفسه، ص131.

رغم أن المشرع لم يحدد في نص المادة شكل الركن المعنوي بصورة واضحة وقاطعة، إلا أن الأصل عند عدم التحديد هو العقاب على الأفعال العمدية حسب القواعد العامة.[1]

وعليه إذا قام المتعامل مع النظام بإعاقة أو إفساد النظام نتيجة لخطأ في التشغيل أو التعامل مع البيانات لم يسأل عن هذه الجريمة.[2]

إذا توافر الركن المعنوي والركن المادي قامت هذه الجنحة واستحق مرتكبها العقوبة المنصوص عليها في م2/323 ق ع ف، وهي العقوبة ذاتها المنصوص عليها في م3/323 ق ع ف.

ويلاحظ أن هذه الجنحة من الجرائم المؤثرة على التجارة الالكترونية، حيث أن هذه التجارة تعتمد على نظم معلوماتية أساسها وسائل إلكترونية، من الوارد جدا أن تتعرض إلى أعمال الإعاقة أو الإفساد، مما يؤثر سلبا على الثقة في التجارة الالكترونية.[3]

ويلاحظ أن المشرع الجزائري لم ينص على جنحة إعاقة أو إفساد نظام المعالجة الآلية للمعطيات للتشابه الكبير بينها وبين جنحة التلاعب بالمعطيات، ذلك أن الأفعال التي تتضمنها هذه الجنحة تؤدي إلى إعاقة النظام وإفساده، كما أن المشرع الجزائري اكتفى بجعل إفساد النظام ظرفا مشددا لجنحة الدخول أو البقاء التي تم التطرق إليها فيما سبق.[4]

[1] غنام محمد غنام، المرجع السابق، ص149.

[2] عبد الحليم رمضان، المرجع السابق، ص55.

[3] بيومي حجازي، المرجع السابق، ص44.

[4] محمد خليفة، المرجع السابق، ص175.

المطلب الرابع: جريمة التلاعب في معطيات الحاسب الآلي.

هذه الجريمة منصوص عليها في م3/323 ق ع ف[1]، وم394 مكرر1 ق ع، ويبدو من خلال هذه المادة أنها جاءت شاملة لكل أنواع المعطيات، وشاملة أيضا لكل وسائل التلاعب بالمعطيات أو بيانات النظام، وعليه يدخل في إطار هذه المادة استخدام الوسائل الخبيثة مهما كانت وسيلة إدخالها إلى الكمبيوتر، ولا يشترط أيضا لقيام جنحة التلاعب أن يكون التلاعب قد تم بعد عملية دخول أو بقاء غير مشروعين، فكثيرا من عمليات التلاعب لا تتم إلا من عاملين مرخص لهم بالدخول إلى النظام.[2]

نصت الاتفاقية العربية لمكافحة جرائم تقنية المعلومات سالفة الذكر في م8 منها على تجريم الاعتداء على سلامة البيانات.[3]

وحتى تقوم جنحة التلاعب لا بد من توافر ركنيها المادي والمعنوي.

الفرع الأول: الركن المادي.

النشاط الإجرامي في هذه الجريمة يتخذ إحدى صور ثلاث وهي: الإدخال، المحو، التعديل، ولا يشترط اجتماع هذه الصور كلها، بل يكفي إحداها لتوافر الركن المادي، ويرِد النشاط الإجرامي في هذه الجنحة على محل محدد هو المعطيات أي المعلومات المعالجة آليا، وليست المعلومات في حد ذاتها، ويقتصر محل النشاط الإجرامي على المعطيات الموجودة داخل النظام أي التي يحتويها وتعتبر جزءا منه، وبناء عليه، لا تقع الجريمة على مجرد المعلومات التي لم يتم إدخالها بعد إلى النظام أو

---

[1] fait d'introduire frauduleusement des données dans un système de traitement automatisé, d'extraire, de détenir, de reproduire, de transmettre, de supprimer ou de modifier frauduleusement les données qu'il contient est puni de cinq ans d'emprisonnement et de 75 000 euros d'amende.
Lorsque cette infraction a été commise à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'Etat, la peine est portée à sept ans d'emprisonnement et à 100 000 € d'amende.

[2] محمد خليفة، المرجع السابق، ص178.

[3] نصت هذه المادة على:

1- تدمير أو محو أو إعاقة أو تعديل أو حجب بيانات تقنية المعلومات قصدا وبدون وجه حق.

2- للطرف أن يستلزم لتجريم الأفعال المنصوص عليها في الفقرة (1) من هذه المادة أن تتسبب في ضرر جسيم.

تلك التي دخلت ولكن لم يتخذ حيالها إجراءات المعالجة الآلية، ويرى جانب من الفقه أن المعلومات التي هي في طريق المعالجة، حتى ولو لم تكن المعالجة الآلية قد بدأت، تكون محلا لجريمة التلاعب.[1]

ولا تقع الجريمة إذا وقع النشاط الإجرامي على المعطيات خارج النظام، سواء قبل دخولها أو بعد خروجها، كما لو كانت مفرغة على قرص أو شريط ممغنط خارج النظام.[2]

ولا يشترط أن تقع صور الفعل الإجرامي المشكل لجنحة التلاعب على المعطيات بشكل مباشر، إذ من الممكن أن يتحقق ذلك بشكل غير مباشر سواء عن بعد أو بواسطة شخص ثالث.[3]

صور السلوك أو النشاط الإجرامي لجنحة التلاعب بمعطيات الحاسب الآلي ثلاث وهي:

أولا: الإدخال.

يقصد بفعل الإدخال إضافة معطيات جديدة على الدعامة الخاصة بها، سواء كانت خالية أم كان يوجد عليها معطيات من قبل. ويتحقق هذا الفعل في كل حالة يتم فيها الاستخدام التعسفي لبطاقات السحب أو الائتمان سواء من صاحبها الشرعي أو من غيره، كحامل البطاقة الذي يستخدم رقمه الخاص للدخول لكي يسحب مبلغا من المال أكثر من المبلغ الموجود في حسابه، كما يتحقق فعل الإدخال في كل حالة يتم فيها إدخال برنامج غريب (فيروس مثلا) يضيف معطيات جديدة.[4]

ثانيا: المحو أو الإزالة.

يقصد بفعل المحو إزالة جزء من المعطيات المسجلة على دعامة والموجودة داخل النظام، أو تحطيم تلك الدعامة، أو نقل وتخزين جزء من المعطيات إلى المنطقة الخاصة بالذاكرة،[5] أو هو

---

[1] عبد القادر القهوجي، المرجع السابق، ص132.

[2] المرجع نفسه، ص133.

[3] المرجع نفسه، ص133.

[4] القهوجي، المرجع السابق، ص133.

من أمثلة الإدخال أيضا:

Faux virement informatique (T.corr. Paris 1998), falsification de bande de payment pour détourner des fonds (T.corr. Thionville 1997). Voir Jean larguier…op cit, p 241.

هذه الحالات يمكن أن تشكل جرائم نصب أيضا، فيعاقب حينها على الجريمة بالعقوبة الأشد، طبقا للقواعد العامة.

[5] عبد القادر القهوجي، المرجع السابق ، ص134.

اقتطاع خصائص مسجلة على دعامة ممغنطة عن طريق إزالتها أو طمسها، أي ضغط خصائص أخرى فوقها، أو عن طريق تحويل ورص خصائص مزالة في منطقة محفوظة من الذاكرة.[1]

ثالثا: التعديل.

يقصد بفعل التعديل تغيير المعطيات الموجودة داخل النظام، واستبدالها بمعطيات أخرى،[2] أو هو تغيير لحالة المعطيات الموجودة بدون تغيير الطبيعة الممغنطة لها، أو هو كل تغيير غير مشروع للمعلومات والبرامج يتم عن طريق استخدام إحدى وظائف الحاسب الآلي.[3]

والجدير ذكره أن الأفعال السابقة من إدخال ومحو وتعديل قد وردت على سبيل الحصر، وعليه يخرج من نطاق هذه الجريمة فعل نسخ المعطيات أو فعل نقلها، أو فعل التنسيق أو التقريب فيما بينها.[4]

من التطبيقات القضائية عن هذه الجريمة، ما قامت به متهمة كانت تعمل في إحدى الشركات، وذلك قبل تركها العمل من إدخال معطيات غير صحيحة تتعلق بمعدل احتساب الضريبة، مما أدى إلى إرباك العمل.[5]

الفرع الثاني: الركن المعنوي.

جنحة التلاعب في المعطيات جريمة عمدية تقوم بالقصد الجنائي العام، لذا يجب لقيامها أن تتجه إرادة الجاني إلى فعل الإدخال أو المحو أو التعديل، كما يجب أن يعلم الجاني بأن نشاطه الإجرامي يترتب عليه التلاعب في المعطيات، ويعلم أيضا بأن لا حق له في القيام بذلك، وأنه يعتدي على صاحب الحق والسيطرة على تلك المعطيات أو أنه يقوم بأفعاله دون موافقته.[6]

---

[1] محمد خليفة، المرجع السابق، ص185.

[2] علي عبد القادر القهوجي، المرجع السابق، ص134.

[3] محمد خليفة، المرجع السابق، ص183.

[4] عبد القادر القهوجي، المرجع السابق، ص134.

[5] Cass. Crim. 5 janv. 1994.

مشار إليه عند: غنام محمد غنام، المرجع السابق، ص153.

[6] عبد القادر القهوجي، المرجع السابق، ص134.

ولا يشترط القصد الخاص لقيام هذه الجريمة، حيث لم يشترط المشرع نية أو قصد الإضرار بالغير، وإن كان وقوع الضرر واردا نتيجة للسلوك الإجرامي، إلا أنه ليس عنصرا من عناصر الجريمة.[1]

وبالنسبة لعقوبة هذه الجريمة فهي الحبس من ستة أشهر إلى ثلاث سنوات والغرامة من 500.000دج إلى 2.000.000دج (م394 مكرر1 ق ع). أما عقوبة الشخص المعنوي فهي خمسة أمثال الحد الأقصى للغرامة المقررة بالنسبة للشخص الطبيعي، أي: 10.000.000دج.

تضاعف العقوبات إذا استهدفت إحدى الجرائم المنصوص عليها الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام، دون الإخلال بتطبيق عقوبات أشد (م394 مكرر3 قانون العقوبات).

وتعاقب م323-3 ق ع ف بالحبس إلى خمس سنوات وبالغرامة المالية مقدرة ب: 75.000 يورو.

جريمة التلاعب بالمعطيات وجريمة إعاقة أو التسبب في تحريف تشغيل نظام معالجة البيانات تهدفان إلى محاربة أفعال التخريب والقرصنة، ولكن ليس من اليسير التمييز بينهما، ذلك أن جريمة إعاقة أو تعطيل النظام وإن كانت تقع بصفة أساسية على البرامج وشبكات الاتصال والنقل، إلا أنها قد تصيب المعطيات أيضا نتيجة أفعال الاعتداء، وبالمقابل فإن الاعتداء على المعطيات الذي تقوم به جريمة التلاعب يؤثر على صلاحية نظام المعالجة الآلية للمعطيات للقيام بوظائفه، سواء على البرامج أو على شبكات الاتصال والنقل، لذلك حاول جانب من الفقه وضع معيار للتفرقة بين الجريمتين، فوضع بعضهم معيار المحل (مادي أو معنوي)، ووضع بعضهم الآخر معيار طبيعة الاعتداء هل هو وسيلة أم غاية، فإذا كان الاعتداء الواقع على المعطيات وسيلة فقط فإن الجريمة هنا هي جريمة إعاقة أو إفساد النظام (م323-2 ق ع ف)، وإذا كان الاعتداء على المعطيات غاية في حد ذاته فإن الجريمة تكون التلاعب في المعطيات أو كما يصطلح عليها جنحة الاعتداء القصدي على المعطيات (م323-3 ق ع ف).

[1] المرجع نفسه، ص135.

ومهما يكن من أمر فإن التفرقة بين الجريمتين لا أهمية لها من الناحية العملية لأن العقوبة المقررة لكل واحدة منهما واحدة، ويخضعان لقواعد عامة واحدة، ولأحكام مشتركة واحدة. [1]

هذه الجرائم تؤثر سلبا على التجارة الإلكترونية، لأنها نمط من أنماط السلوك الإجرامي الذي يقع على التجارة الإلكترونية.[2]

المطلب الخامس:جريمة التعامل في معطيات غير مشروعة

نصت على هذه الجريمة م394 مكرر2 ق ع، وذكرت العديد من الصور، وتقابلها م323-3/1 ق ع ف،[3] ويعتبر النص على هذه الجريمة عقبة في وجه المجرمين لمنعهم من ارتكاب الجرائم المنصوص عليها في القسم المتعلق بالمساس بأنظمة المعالجة الآلية للمعطيات، و يظهر هذا الأمر جليا إرادة المشرع ورغبته في إضفاء حماية إضافية، وبطريقة غير مباشرة لأنظمة المعالجة الآلية للمعطيات.[4]

وقد أشارت المذكرة التفسيرية لاتفاقية بودابست إلى الحكمة من تجريم هذه الأفعال بقولها: "إن جرائم المعطيات يُتطلب لارتكابها حيازة وسائل الولوج، كأدوات القرصنة أو أي أدوات أخرى، وأن هناك دافعا قويا للحصول على هذه الوسائل لأغراض إجرامية، مما قد يؤدي إلى إيجاد نوع من السوق السوداء لإنتاج وتوزيع مثل هذه الأدوات، ومن أجل وقاية أكثر فعالية من هذه المخاطر، فإنه يجب على قانون العقوبات أن يحظر الأفعال راجحة الخطورة من المنبع، قبل ارتكاب الجرائم المنصوص عليها في المادتين 02 و 05".[5]

على ضوء نص م323-3/1 ق ع ف عاقبت محكمة استئناف مدينة "مونت بولييه" الفرنسية عملية نشر قام بها أحد الخبراء على الانترنت لقوانين استغلال " codes

---

[1] القهوجي، المرجع السابق، ص136.

[2] بيومي حجازي، المرجع السابق، ص55.

[3] Le fait, sans motif légitime, notamment de recherche ou de sécurité informatique, d'importer, de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou toute donnée conçus ou spécialement adaptés pour commettre une ou plusieurs des infractions prévues par les articles 323-1 à 323-3 est puni des peines prévues respectivement pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée.

[4] Renaud Salomon, op cit, p216.

[5] محمد خليفة، المرجع السابق، ص194.

d'exploitation" الثغرات غير المصححة، وادعى الناشر في دفاعه بأن له دافعا أو مسوغا شرعيا "motif légitime" هو إعلام وتحسيس الجمهور وكذا المختصين المعنيين بمشاكل الحماية الفنية، بغية إيجاد حلول لها، فحسبه إن اختراقه للأنظمة الفنية للحماية دليل على عدم كفاءتها، غير أن القضاة لم يلتفتوا لدفاعه هذا واعتبروا أن نشر مثل هذه المعلومات يمكن أن يشكل خطرا عند استعمالها لأغراض القرصنة من قبل الجمهور المميز الذي يبحث عن هذا النوع من المعلومات لاختراق الأنظمة الفنية، وهذا ما أكدته محكمة النقض الفرنسية.[1]

وقد نصت الاتفاقية العربية لمكافحة جرائم تقنية المعلومات سالفة الذكر تحت مسمى "جريمة إساءة استخدام وسائل تقنية المعلومات" على هذه الجريمة في م9 منها.[2]

بناء على ما تقدم فإن هذه الجريمة لا تقوم إلا بتوافر ركنيها: المادي والمعنوي.

الفرع الأول: الركن المادي لجريمة التعامل في معطيات غير مشروعة

نص المشرع الجزائري في م394 مكرر1/2 ق ع، على تجريم تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة أو مراسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها في القسم المتعلق بالمساس بأنظمة المعالجة الآلية للمعطيات، ويشكل فعل التصميم[3] أو البحث[4] أو التجميع[1] أو التوفير[2] أو النشر،[3] أو الاتجار في معطيات مخزنة

---

[1] Crim.27 oct. 2009, voir: Christiane Féral-SCHUHL, op cit, p924.

[2] تنص هذه المادة على تجريم كل من:

1- إنتاج أو بيع أو شراء أو توزيع أو توفير:

أ) أية أدوات أو برامج مصممة أو مكيفة لغايات ارتكاب الجرائم المبينة في م6 إلى م8.

ب) كلمة سر نظام معلومات أو شيفرة دخول أو معلومات مشابهة يتم بواسطتها دخول نظام معلومات ما بقصد استخدامها لأية من الجرائم المبينة في 6 إلى م8.

2- حيازة أية أدوات أو برامج مذكورة في الفقرتين أعلاه، بقصد استخدامها لغايات ارتكاب أي من الجرائم المذكورة في 6 إلى م8.

[3] التصميم هو أول عملية في سلسلة التعامل في المعطيات، وهي تتمثل في إخراج المعطيات إلى الوجود أي القيام بإنشاء وإيجاد معطيات صالحة لارتكاب جريمة، وهذا العمل يقوم به المختصون في هذا المجال كالمبرمجين ومصممي البرامج، ومثال هذه الجريمة تصميم برنامج يحمل فيروسا، وهذا ما يطلق عليه بالبرامج الخبيثة، أو تصميم برنامج اختراق. محمد خليفة، المرجع السابق، ص200.

[4] يتساءل البعض عن المقصود من البحث في نص م394 مكرر2، هل هو البحث عن المعطيات التي يمكن أن ترتكب بها الجريمة، أم هو البحث في كيفية تصميم هذه المعطيات؟

وبالمنظور الأول: هل يعتبر من يشغل أحد محركات البحث الموجودة على شبكة الانترنت لتقوم بالبحث عن مواقع تعليم كيفية القيام باختراق أجهزة الحاسب الآلي، هل يعتبر هذا السلوك في حد ذاته جريمة. لا ينبغي التوسع في تفسير هذه العبارة، فما من شك أن التفسير السابق من شأنه أن يوسع كثيرا من نطاق التجريم، لأن الأصل أن البحث عن الوسيلة التي يمكن أن ترتكب بها الجريمة لا يعد في حد ذاته جريمة، ومن شأن هذا التعبير إذا أسيء

أو معالجة أو مراسلة عن طريق منظومة معلوماتية[4] النشاط الإجرامي المشكل للركن المادي لهذه الجريمة، كما أن حيازة[5] أو إفشاء[1] أو نشر[2] أو استعمال لأي غرض كان (حتى ولو كان نبيلا)

تفسيره أن يشكل تهديدا صريحا للحريات، وبناء عليه فالأرجح أن المشرع يقصد البحث في كيفية تصميم هذه المعطيات وإعدادها، وليس مجرد البحث عن المعطيات. محمد خليفة، المرجع السابق، ص201.

[1] التجميع هو القيام بجمع العديد من المعطيات التي يمكن أن ترتكب بها الجرائم محل الدراسة، ويفترض هنا أن الفاعل يحتفظ بمجموعة من المعطيات التي تشكل خطرا والتي من الممكن استعمالها في ارتكاب تلك الجرائم، وقدر المشرع، أن تعدد المعطيات من شأنه أن يرفع درجة الخطر التي تشكلها، فما من شك أن من يجوز معطيات واحدة لا يشكل خطرا بقدر ما يشكله من يقوم بتجميع هذه المعطيات، إذ أن التجميع يعكس خطورة الفاعل ويشير إلى إمكانية ارتكابه أو تسهيله لارتكاب إحدى جرائم المعطيات.

ولا يستخدم قانون العقوبات الفرنسي الجديد (2004) في مادته 323-3-1 مصطلح التجميع بل يستخدم مصطلح التجميع بل يستخدم مصطلح الحيازة، وكذلك الشأن مع اتفاقية بودابست لعام 2001، ولا شك أن التجميع يقتضي الحيازة وإن كان أيضا يقتضي وجود عدد من المعطيات- أي مجموعة- ولا يقوم بحيازة معطيات واحد.

وقد استخدمت اتفاقية بودابست مصطلح "الحصول للاستخدام" وما يميز هذا المصطلح عن مصطلح التجميع أن الأول يقتضي وجود نية استخدام المعطيات المتحصل عليها ولا يشترط عددا معينا فيها. بينما الثاني- التجميع- لا يشترط مثل تلك النية ويشترط تعدد المعطيات.

[2] من الأفعال التي تجرمها المادة 394 مكرر 02 من قانون العقوبات الجزائري أيضا فعل التوفير، أي توفير معطيات تمكن أن ترتكب بها جريمة دخول أو بقاء أو جريمة تلاعب، وتعاقب المادة 323-3-1 على نفس السلوك تحت مصطلح ceder كما تعاقب عليه المادة السادسة من اتفاقية بودابست تحت عبارة "أي أشكال للوضع تحت التصرف"، والحقيقة أن الترجمة الفرنسية للمادة 394 مكرر 02 من قانون العقوبات الجزائري توافق هذه العبارة وهي " الوضع تحت التصرف" والمراد من ذلك تقديم المعطيات وإتاحتها لمن يريدها، أي جعلها في متناول الغير، ووضعها تحت تصرفه.

والفرق بين التوفير والتجميع أنه في هذا الأخير لاتتعدى حيازة المعطيات والتصرف فيها على من يقوم بالتجميع، بينما في التوفير فإن دائرة الأشخاص الذين سيحصلون على المعطيات ويتصرفون فيها تتعدي ذلك الشخص وتتسع بذلك وتزيد الخطورة بازدياد هؤلاء.

هذا ويستخدم المشرع الفرنسي في المادة سابقة الذكر مصطلح mettre à disposition، وهو يعني الوضع تحت التصرف، وتوافقه الترجمة الفرنسية لمصطلح توفير في قانون العقوبات الجزائري. محمد خليفة، المرجع السابق، ص203.

[3] المقصود بالنشر إذاعة المعطيات محل الجريمة، بتمكين الغير من الاطلاع عليها عن طريق مختلف وسائل النشر المختلفة ومنها الانترنت، ونصت على النشر م6 من اتفاقية بودابست، ولم ينص قانون العقوبات الفرنسي على فعل النشر. والنشر من أخطر الأفعال التي ترد على المعطيات المجرمة، باعتباره سلوكا ناقلا للمعطيات المجرمة إلى عدد كبير من الأشخاص، فيزداد بالنتيجة احتمال استعمال هذه المعطيات. المرجع السابق، ص203.

[4] الاتجار بالمعطيات هو تمكين الغير منها لقاء مقابل أيا كان، والاتجار يشمل كل التعاملات التي تقع على المعطيات الصالحة لارتكاب جريمة من جرائم المساس بالمعطيات بمقابل، والفرق بين الاتجار والتوفير أن هذا الأخير قد يكون دون مقابل. ولا يقصد بالاتجار في م394 مكرر2 المفهوم الوارد في القانون التجاري، بل تشمل كافة الأفعال بمقابل ولو لم ينص عليها القانون التجاري ضمن الأعمال التجارية التي ينظمها. وجاء النص الفرنسي خاليا من هذا المصطلح، وخلت منه أيضا اتفاقية بودابست، بل تضمنت مصطلح "البيع والاستيراد"، وتضمن النص الفرنسي مصطلح الاستيراد، والظاهر أن المشرع الفرنسي لا يعير اهتماما للمقابل فتقديم المعطيات مجرم سواء أتم مجانا أم بمقابل. محمد خليفة، المرجع السابق، ص204.

[5] الحيازة في إطار القانون الجزائي رابطة واقعية بين شخص ومال تتيح للأول أن يسيطر على الثاني سيطرة مستقلة مقترنة بنية الاحتباس وتكون السيطرة على المال مستقلة إذا كان يمكن للشخص أن يمارس أي عمل مادي على الشيء بدون رقابة من شخص آخر له على المال سلطة قانونية أعلى بمقتضي حق من الحقوق.

فلا يعتبر حائزا العامل الذي تربطه علاقة العمل بالمعطيات، لأنه لا يسيطر عليها بنية الاحتباس، ولا يمكنه أن يمارس أي عمل عليها بدون تصريح من رب العمل.

والحيازة في القانون الجنائي ليست حقا، بل هي مركز واقعي، وعليه يمكن أن تكون مشروعة تستند إلى سبب صحيح قانونا كما يمكن أن تكون غير مشروعة، ولكنها في جريمة التعامل في معطيات غير مشروعة تكون دائما غير مستندة لسبب شرعي ذلك أنه يشترط أن تكون متحصلة من إحدى جرائم المعطيات سواء كانت جريمة دخول أو بقاء غير مصرح بهما أو كانت جريمة تلاعب بالمعطيات.

المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في القسم المتعلق بالمساس بأنظمة المعالجة الآلية للمعطيات،[3] يشكل بدوره النشاط الإجرامي الذي يقوم به الركن المادي لهذه الجريمة في صورتها الثانية حسب نص م394 مكرر2/2 ق ع.

هذه الجريمة هي من جرائم السلوك المجرد، أي جريمة خطر وليست جريمة ضرر، شأنها في ذلك شأن جريمة الدخول غير المشروع إلى STAD.

والملاحظ من خلال نص هذه المادة أن المشرع قد حمى المعطيات بنوعيها المخزنة، والمعالجة آليا، ومن هذه المعطيات المخزنة ما يعرف ببنوك المعلومات، وهي مجموعة البيانات أو المعلومات المخزنة في جهاز الحاسب الآلي بقصد معالجتها إلكترونيا، وقد غدت هذه الوسيلة ميزة العمل التقني المتقدم للأفراد والمؤسسات، نتيجة لتطور الأنظمة المعلوماتية، وتختلف هذه المعلومات

كما أن الحيازة لا تقوم إلا بسيطرة الحائز على المعطيات، بحيث يكون باستطاعته التأثير عليها تأثيرا يتفاوت حجمه تبعا لنوع الحيازة، إذ قد تكون السيطرة مطلقة يستطيع معها الحائز أن يفني المعطيات أو يعدل فيها أو يستعملها، كما قد تكون هذه السيطرة من الناحية الواقعية محدودة تمكنه فقط من الانتفاع بالمعطيات أو استغلالها في وجه معين، وعليه يكفي للقول بتوافر السيطرة مجرد استطاعة هذه السيطرة دون عقبات واقعية تحول بين الشخص وبين التمتع بها.

ولا تكفي مجرد سيطرة الحائز على المعطيات لكي تقوم الحيازة بل يلزم أن تكون هذه السيطرة إرادية أي أنها مقترنة بنية احتباس المعطيات والسيطرة عليها وهذا لا يتحقق إذا كان تمتع الحائز بسلطاته على المعطيات لم يكن إلا أمرا عرضيا أو جدته المصادفة أو تم بنية عدم التكرار، لأنه يلزم أن تكون سيطرة الشخص على المعطيات مقترنة بنية احتباسها على الدوام أو لمدة معينة. ومادامت نية الاحتباس ركنا أصليا من أركان الحيازة فإن العلم بكنه المعطيات المتحصلة من جريمة وبدخولها في نطاق السيطرة لازم لا تقوم الحيازة بدونه، لأنه من لا يعلم لا يحوز. المرجع السابق، ص206.

[1] الإفشاء تتمتع الحاسبات الآلية بقدرة هائلة على تخزين المعلومات مما جعلها مستودعا لأهم المعلومات وأكثرها حساسية سواء كانت متعلقة بمصالح الدولة أو تعلقت بالأفراد أو بالمصالح الاقتصادية لمختلف المؤسسات أو تعلقت بالمجالات العلمية، ومع ازدياد أهمية هذه المعلومات وكثرة الاعتماد على تخزينها داخل أنظمة الحاسبات تزداد المخاوف من الحصول عليها بطريقة غير مشروعة عن طريق اختراق تلك الأنظمة ثم القيام بإفشائها لتحقيق مصالح عديدة.

ولذلك قامت العديد من التشريعات بتجريم الإفشاء غير المشروع ق ع جزائري للمعطيات التي يتحصل عليها بطريقة غير مشروعة، فقد قامت المادة 394 مكرر 02 من قانون العقوبات الجزائري في بندها الثاني بتجريم إفشاء المعطيات المتحصلة من جريمة دخول أو بقاء غير مصرح بهما أو من جريمة تلاعب.

بينما لا يتضمن قانون العقوبات الفرنسي مثل هذا النص، إذ لا يعاقب على هذا الفعل في القانون الفرنسي. المرجع نفسه، ص207.

[2] فعل النشر هو الفعل الوحيد المشترك بين صورتي جريمة التعامل في معطيات غير مشروعة، ومن صور النشر ما يقوم به المخترقون من اختراقات لمواقع معينة وحصولهم على كلمات العبور فيها والقيام بنشرها ليعلمها الجميع لدوافع مختلفة. ولم تشترط المادة عددا معينا من المرات التي يتم النشر فيها كما لم تحدد أن يكون النشر بمقابل أو بالمجان، كما لم تحدد وسيلة معينة للنشر. المرجع نفسه ص209.

[3] لم يفت المشرع أن يجرم الاستعمال باعتباره أخطر سلوك يمكن أن يقع على المعطيات المتحصلة من جريمة، كأن تقوم شركة ما باستعمال معطيات أو معلومات تخص شركة منافسة، متحصل عليها بطريقة غير مشروعة، ويشمل هذا التجريم كل استعمال لهذه المعطيات مهما كان الهدف منه أو الدافع له، ومن أمثلة الاستعمال استخدام كلمة العبور التي تم الحصول عليها إثر دخول غير قانوني. المرجع نفسه، ص210.

المخزنة باختلاف الموضوعات المتعلقة بها، وقد يتم تخزينها على موقع معين يتم إنشاؤه على شبكة الانترنت،[1] ومن دون شك فإن هذه المعلومات المخزنة يجب أن تتوفر فيها مجموعة من الشروط كأن تكون متعلقة بمؤسسة وطنية مهمة وحساسة كمؤسسات الدفاع الوطني، أو أن تمس بخصوصية الأفراد،[2] أو أن تكون معلومات مميزة في المجال التجاري أو المالي...

ولم يقصر المشرع الفرنسي محل الجريمة على المعطيات، بل امتد ليشمل كل الوسائل المعدة والمصممة خصيصا لأن تستخدم في ارتكاب الجرائم المنصوص عليها في المواد 323-1 إلى 323-3 ق ع ف، لكن المشرع الجزائري – على عكس المشرع الفرنسي وما جاء في اتفاقية بودابست– لم يتطلب أن تكون هذه المعطيات مخصصة لارتكاب الجريمة، حيث يكفي أن تكون صالحة لأن ترتكب بها الجريمة.[3]

الفرع الثاني: الركن المعنوي لجريمة التعامل في معطيات غير مشروعة

جريمة التعامل في معطيات غير مشروعة جريمة عمدية، بنص م394 مكرر2 "عمدا وعن طريق الغش"، يلزم لتوافرها القصد الجنائي العام بعنصريه العلم والإرادة، علم الفاعل بأنه يتعامل في معطيات غير مشروعة، وانصراف إرادته رغم ذلك لارتكاب النشاط الإجرامي.

ويرى البعض أن المشرع يتطلب إلى جانب القصد العام قصدا خاصا يتمثل في نية الإعداد أو التمهيد لاستعمال هذه المعطيات، وهذا بالنسبة للصورة الأولى لهذه الجريمة المنصوص عليها في الفقرة الأولى من م394 مكرر2 "تجريم تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة أو مراسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها في القسم المتعلق بالمساس بأنظمة المعالجة الآلية للمعطيات"، وهذا يتوافق مع مبادئ العدالة وما جاءت به اتفاقية بودابست في هذا الشأن، أما بالنسبة للصورة الثانية المنصوص عليها في الفقرة الثانية من المادة سالفة الذكر فإن استعمال المشرع لمصطلح "لأي غرض كان" يقطع الطريق أمام أي تأويل، ويوضح بجلاء أن المشرع لا يتطلب بالنسبة لهذه الجريمة "حيازة أو إفشاء أو

[1] زيدان زيبحة، الجريمة المعلوماتية في التشريع الجزائري والدولي، دار الهدى، عين مليلة، الجزائر2011، ص57.

[2] المرجع نفسه، ص58.

[3] محمد خليفة، المرجع السابق، ص198.

نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في القسم المتعلق بالمساس بأنظمة المعالجة الآلية للمعطيات" سوى القصد الجنائي العام، ولا يتطلب قصدا جنائيا خاصا.[1]

أما المشرع الفرنسي فلم يستعمل لفظ "عمدا وعن طريق الغش"، وإنما أورد لفظا آخر هو "مسوغ شرعي"، مما يجعل الركن المعنوي بالنسبة لهذه الجريمة مقتصرا على القصد الجنائي العام وحده فقط، دون القصد الخاص.[2]

بالنسبة للعقوبة، الملاحظ أن المشرع الجزائري قد خص هذه الجنحة بأكبر عقوبة في جانبها المالي (الغرامة من مليون إلى خمسة ملايين دينار)، وبناء على نص هذه المادة، وعلى نص م394 مكرر 4، فإن عقوبة الشخص المعنوي المرتكب لهذه الجنحة تصل إلى 25 مليون دينار.

أما المشرع الفرنسي فقد جعل العقوبة على هذه الجريمة هي عقوبة الجريمة ذاتها التي صممت الوسائل أو أعدت لارتكابها، أو عقوبة الجريمة الأشد في حالة التعدد المعنوي للجرائم.

[1] محمد خليفة، المرجع السابق،ص ص211-218.

[2] المرجع نفسه، ص219.

المبحث الثاني: الحماية الجزائية لحقوق الملكية الفكرية المتعلقة بالتجارة الالكترونية.

يتم تناول هذا المبحث من خلال دراسة حماية محتويات المواقع المخصصة للتجارة الالكترونية، في ضوء قوانين الملكية الفكرية (المطلب الأول)، ثم من خلال حماية أسماء الحقول التجارية على شبكة الانترنت، أو ما يطلق عليه أيضا أسماء النطاق (المطلب الثاني)، باعتبار أن موضوع الملكية الفكرية يتم تقسيمه في الغالب إلى حقوق المؤلف، وحقوق الملكية الصناعية.

المطلب الأول: الحماية الجزائية لمحتويات مواقع التجارة الالكترونية في ضوء قوانين حماية الملكية الفكرية.

يعالج هذا المطلب من خلال علاقة التجارة الالكترونية بالملكية الفكرية (الفرع الأول)، والحماية التي توفرها قوانين حماية الملكية الفكرية (الفرع الثاني)، وحماية المصنفات في ظل قانون حقوق المؤلف والحقوق المجاورة (الفرع الثالث).

الفرع الأول: علاقة التجارة الالكترونية بالملكية الفكرية.

تعتبر الملكية الفكرية من مجالات القانون التي تتناول حقوق الملكية الخاصة بالأمور المعنوية، من خلال حماية الإبداعات العقلية الجديدة، وتشجيع المعاملات التجارية الشريفة، وتعزيز تلبية حاجات المستهلك من خلال تنظيم أوجه بعض الممارسات التجارية.

تسمى حقوق الملكية الفكرية بالحقوق الذهنية، وهي نوعان: حقوق ناشئة عن الملكية الأدبية والفنية، وتعرف بحقوق المؤلف والحقوق المجاورة أو المرتبطة، وحقوق ناشئة عن الملكية الصناعية.[1]

[1] د. حسام محمود لطفي، حقوق الملكية الفكرية، ط2، القاهرة 2012 (دون ذكر دار النشر)، ص1.
وقد تطرقت المادة الأولى من اتفاقية باريس لهذه الحقوق الناشئة عن الملكية الصناعية، وتجد تطبيقات لها في مجال براءات الاختراع، والرسم، والنموذج الصناعي، والعلامة التجارية، والاسم التجاري، والعنوان التجاري، والبيانات التجارية، والمعلومات غير المفصح عنها، والأصناف النباتية، والتصميمات التخطيطية للدوائر المتكاملة، والمؤشرات الجغرافية، وأسماء الدومين (أسماء المجال أو أسماء النطاق).المرجع نفسه ص7.

وتتمتع هذه الحقوق كلها بالحماية شريطة الأصالة أو الابتكار[1] (originalité)إذا تعلق الأمر بحق من حقوق المؤلف والحقوق المجاورة،[2] بالإضافة إلى الجدة والقابلية للتصنيع إذا اندرج الحق ضمن حقوق الملكية الصناعية.[3]

وقد أثرت تقنية المعلومات بشكل كبير على مختلف حقول الملكية الفكرية، خاصة فيما يتعلق بتوفير الحماية للمصنفات الجديدة (المصنفات الرقمية)،[4] أو توفير الحماية للمصنفات المعروفة بسبب ما أتاحته التقنية الحديثة من سهولة الاعتداء عليها.

وبالنسبة للتجارة الالكترونية، فإنها تتطلب أكثر من غيرها بيع منتجات وتوفير خدمات قائمة على الملكية الفكرية وترخيصها، حيث أن التجارة الالكترونية تمتد إلى الموسيقى والرسوم والصور وبرامج الكمبيوتر...وهذا يتطلب حماية لهذه المبيعات عن طريق قوانين حقوق الملكية الفكرية، وإلا تظل عرضة للسرقة أو القرصنة، مما قد يؤدي إلى انهيار المشروع التجاري برمته.[5]

كما أن النظم التي تقوم عليها التجارة الإلكترونية تعتبر جوانب في الملكية الفكرية التي غالبا ما توفر لها الحماية، كبرامج الكمبيوتر، والشبكات والتصميمات، ورقائق الكمبيوتر، والمحولات...

---

[1] يستعمل الفقه المصري في غالبيته مصطلح الابتكار، بينما يحبذ فقهاء الجزائر ولبنان استخدام مصطلح أصالة للتعبير عن مصطلح originalité، وهو المصطلح الأقرب للصواب كما تدل عليه المعاجم اللغوية، ونجد أيضا فقهاء آخرين يستخدمون مصطلح إبداع.

[2] سميت الحقوق المجاورة بهذا الاصطلاح لتجاورها مع حقوق المؤلف وارتباطها معه، وتشمل حقوق المؤدين والمنتجين وهيئات البث الاذاعي والتلفزي. انظر: د. عبد الله عبد الكريم عبد الله، الحماية القانونية لحقوق الملكية الفكرية على شبكة الانترنت، دار الجامعة الجديدة، الإسكندرية، مصر، 2009، ص18.

[3] د. محمود عبد الرحيم الديب. الحماية القانونية للملكية الفكرية في مجال الحاسب الآلي والانترنت، دار الجامعة الجديدة، الإسكندرية، مصر 2005، ص26.

[4] لم تعرف معظم التشريعات المصنف الرقمي، تاركة هذه المهمة للفقه الذي وجد صعوبة في تعريفه، ورغم ذلك اجتهد الفقهاء من أجل وضع تعريف له، ومن ذلك تعريف المصنف الرقمي على أنه: "مصنف إبداعي عقلي، ينتمي إلى بيئة تقنية المعلومات، ويضم برامج الحاسوب وقواعد البيانات والدوائر المتكاملة وأسماء نطاقات ومواقع الانترنت... " وقد تطرق المشرع الجزائري في م 04و م05 من الأمر 05/03 إلى برامج الحاسوب وقواعد البيانات وباقي المصنفات التي تماثلها، مما حذا بالبعض إلى القول أن المشرع الجزائري قد أورد هذه المصنفات على سبيل المثال لا الحصر. انظر: راضية مشري، الحماية الجزائية للمصنفات الرقمية في ظل قانون حق المؤلف، مجلة التواصل في العلوم الإنسانية والاجتماعية، عدد 34، جوان 2013، ص 137. وانظر أيضا: حواس فتيحة، حماية المصنفات المنشورة على الانترنت، مذكرة ما جستير، فرع الملكية الفكرية، كلية الحقوق، جامعة الجزائر، 2004، ص07 وما بعدها.

[5] أمين أعزان، المرجع السابق، ص293.

ويثير محتوى موقع الانترنت جدلا واسعا، فهل تُحمى محتوياته ككتلة واحدة ضمن مفهوم قانون حق المؤلف، أم تفصل هذه العناصر ليسند اسم الموقع إلى الأسماء التجارية، وشعار الموقع إلى العلامات التجارية، والنصوص والموسيقى والرسوم إلى قانون حق المؤلف كمصنفات أدبية؟

الفرع الثاني: الحماية التي توفرها قوانين حماية الملكية الفكرية.

حتى يجوز قانونا أن تتواجد بمواقع الانترنت أعمال أيا ما كانت طبيعتها (صور، أعمال موسيقية، رموز...) يجب أن يوافق أصحاب الحقوق مهما كانوا (مؤلفون، منتجون، فنانون...) على هذه الأعمال، مع عدم الإخلال بحق المستخدم في الاستعانة بمقتطفات قصيرة من هذه الأعمال لأغراض نقدية أو تعليمية أو علمية أو إشهارية مع ضرورة الإشارة إلى صاحب العمل ومصدره.[1]

والسؤال المطروح بالنسبة لقوانين حماية المصنفات الأدبية والفنية هو: هل تكفي القوانين القائمة لحماية الأعمال المستحدثة التي تعد خصيصا لإنشاء موقع على الانترنت وتستخدم فيها التكنولوجيا الرقمية، أم أن هذه القوانين في حاجة إلى تغيير أو تعديل؟ ويبرز سؤال آخر مرتبط بسابقه هو: هل تشمل الحماية تكنولوجيا الوسائط المتعددة "Multimédia"؟ وهي تلك التكنولوجيا التي تسمح باجتماع النصوص والموسيقى والصور والأفلام والفيديو...كلها أو البعض منها كما تسمح بتعامل أكثر من شخص معها.[2]

تناول مشروع الاتفاقية المعلن في شأن التجارة الإلكترونية عن المجلس الأوربي في 27 أفريل 2000 في المادة العاشرة منه جريمة الاعتداء على الملكية الفكرية والجرائم الملحقة بها، حيث حث الدول المتعاقدة على أن تجرم في قوانينها الداخلية التقليد والتوزيع بطريق أنظمة الكمبيوتر الأعمال المحمية بقوانين الملكية الفكرية وفقا للقانون الوطني، استنادا إلى اتفاقية برن لحماية الأعمال الأدبية والفنية، واتفاقية "التربس" ومعاهدة "الويبو" للملكية الفكرية، إذا ارتكبت هذه الأفعال بصورة الاتجار عمدا ودون حق، وأجاز المشروع لأي طرف من الأطراف تجريم تقليد وتوزيع بواسطة نظام للكمبيوتر أعمال أو اختراعات محمية وفقا لقانون الدولة واستنادا لمعاهدة برن بشأن الأداء والفونوجرام.[3]

---

[1] مدحت عبد الحليم رمضان، المرجع السابق، ص57.

[2] المرجع نفسه، ص58.

[3] المرجع نفسه، ص59.

إذا كان العمل المراد حمايته قطعة موسيقية أو رسما أو عملا أدبيا أو برنامجا للكمبيوتر فلا تثور مشكلة كبيرة حسب بعض الفقه، فقد طبق كل من القضاء الأمريكي والقضاء الفرنسي النصوص الخاصة بحماية الملكية الفكرية على أفعال تقليد قام بها البعض على الانترنت.[1]

ولكن إذا تم تجميع هذه المجموعة من الأعمال أو بعضها لإخراج صفحة أو موقع على الانترنت، كموقع للتجارة الالكترونية، فإن الأمر يصبح دقيقا، حيث أن قوانين الملكية الفكرية لا تحمي العمل متعدد الوسائط في ذاته.

ذهب جانب من الفقه الفرنسي قبل تعديل قانون الملكية الفكرية الفرنسي، إلى أن قانون الملكية الفكرية يشمل بالتأكيد حماية الأعمال متعددة الوسائط طالما أنها تتسم بالابتكار أو الأصالة، والأعمالُ المتعددة الوسائط تقوم على استخدام مجموعة من المعطيات وبالتالي فهي تقوم على الابتكار.[2]

وانتهى جانب من الفقه الفرنسي إلى أن الأعمال التي تقوم على الوسائط المتعددة والتي تعد منها مواقع الانترنت، تدخل في نطاق قواعد البيانات التي شملها قانون الملكية الفكرية بالحماية (القانون رقم 36/98 الصادر في فاتح جويلية 1998)، والذي عرف قاعدة البيانات بأنها مجموعة من الأعمال أو المعطيات أو العناصر المستقلة والموضوعة بطريقة منتظمة أو منطقية ويمكن للشخص الوصول إليها بالوسائل الإلكترونية، أو بأية وسيلة أخرى.

لذلك فإن هذا التعريف الواسع يسمح بتطبيقه على مواقع شبكة الانترنت التي تسمح فكرتها الفنية بالتعامل المستقل، كما أن تطور هذه المواقع أدى إلى أنها صارت تتخذ شكل قواعد البيانات، وهذا الرأي يتفق مع الاتجاه الأوربي الذي يعتبر قواعد البيانات من الأعمال التي تشملها بالحماية قوانين الملكية الفكرية.[3]

---

[1] اعتبر القضاء الأمريكي قيام البعض بوضع صور خاصة بإحدى المجلات على الانترنت دون موافقة المجلة بما يسمح للبعض بإنزال الصور ونسخها، تقليدا. كما اعتبر القضاء الفرنسي وضع قطع موسيقية لأحد المغنين على الانترنت دون موافقة أصحاب الحق مكونا لجريمة التقليد. يراجع: عبد الحليم رمضان، المرجع السابق، ص59.

[2] المرجع نفسه، ص60.

[3] المرجع نفسه، ص61.

وفي الجزائر فإن المشرع نص في م3 من الأمر 05/03 المؤرخ في 19 يوليو 2003 المتعلق بحقوق المؤلف والحقوق المجاورة،[1] على منح الحماية للمصنف مهما يكن نوعه، ونمط تعبيره، ودرجة استحقاقه ووجهته، سواء أكان المصنف مثبتا أم لا بدعامة تسمح بإبلاغه إلى الجمهور، شرط إيداعه، كما أن م4/أ نصت صراحة على برنامج الحاسوب، وم5 من القانون ذاته نصت على قواعد البيانات باعتبارها مصنفا جديرا بالحماية، سواء أكانت مستنسخة على دعامة قابلة للاستغلال بواسطة آلة أو بأي شكل من الأشكال الأخرى.

عربيا، نصت كل من المادة الثانية، والمادة الرابعة من قانون حماية حق المؤلف المصري، القانون رقم 38 لسنة 1992 على اعتبار برامج الحاسب الآلي وقواعد البيانات من المصنفات الأدبية، كما أعطي وزير الثقافة سلطة إضافة مصنفات أخرى تماثلها، كما أن م4 تقرر حماية للعمل المركب إذا كان مبتكرا أو متميزا في ترتيبه، أو لمجهود شخصي.

وعاقب المشرع المصري على تقليد المصنفات الأدبية ومن بينها برامج الكمبيوتر وقواعد البيانات وفقا لنص م47 من قانون حماية حق المؤلف، وبناء على هذا النص يعد مرتكبا لجريمة التقليد كل من يقوم بتقليد موقع للانترنت أو التعديل أو التحوير فيه دون موافقة صاحبه.[2]

وبعد تعديل قانون حماية حق المؤلف المصري بالقانون 82 لسنة 2002 نصت م2/140 على برامج الحاسب الآلي، وم3/140 على قواعد البيانات سواء كانت مقروءة من الحاسب الآلي (الكمبيوتر) أو من غيره، واستبعدت دور وزير الثقافة في هذا المجال.

الفرع الثالث: جنحة التقليد والجنح الشبيهة بها.

اهتمت القوانين المتعلقة بحماية الملكية الفكرية بالنص على حماية المصنفات المختلفة بما في ذلك قواعد البيانات وبرامج الحاسب الآلي باعتبارها من حقوق المؤلف، ولم تشترط لذلك سوى شرطين:[3] الأصالة، وتعني تمييز المصنف عن غيره من المصنفات التي تكون في المجال نفسه، بحيث يبرز

---

[1] ج ر44 لسنة 2003. وقد ألغت م163 من هذا الأمر صراحة الأمر رقم 10/97 المتعلق بحقوق المؤلف والحقوق المجاورة.

[2] عبد الحليم رمضان، المرجع السابق، ص65.

[3] نقصد هنا الشروط الخاصة لحماية المصنفات، إذ يوجد شرطان عامان لا بد من توافرهما حتى يحظى المصنف بالحماية وهما وجود المصنف حسب قواعد القانون المدني، وعدم مخالفته للنظام العام. انظر: بن زيطة عبد الهادي، حماية برامج الحاسوب في التشريع الجزائري، دار الخلدونية، الجزائر 2007، ص37 وما بعدها.

شخصية صاحبه، سواء أكان ذلك في مضمون الفكرة وجوهرها، أو في الطريقة المتبعة لعرض هذه الفكرة،[1] وشرط شكلي يقضي بأن يتم إخراج العمل إلى حيز الوجود أيا كانت صورة هذا الإخراج، وتتطلب بعض القوانين، ومنها القانون الجزائري، الإيداع القانوني للمصنف، ومعنى ذلك إلزام صاحب الحق على المصنف بتسليم نسخة أو أكثر منه لإحدى السلطات الحكومية أو إحدى المكتبات الخاصة التي يحددها القانون لهذا الغرض كشرط شكلي لتمتعه بالحماية القانونية ضد أي اعتداء.[2]

ولحماية المصنفات أيا كان نوعها أهمية كبيرة، ذلك أن هذه الحماية تشجع مبدعيها على نشرها والاستفادة المالية والأدبية منها، بدل الاحتفاظ بها خوفا من التعدي عليها، وهذا يؤدي إلى خلق جو من المنافسة الإبداعية، والقضاء أو الحد من قرصنتها أو تقليدها لما تشكله من اعتداء على حقوق المبدعين.[3]

ومن أهم أنواع الحماية التي أقرها المشرع في قانون حماية المؤلف، النص على تجريم التقليد، والجرائم المشابهة له.

أولا: جريمة التقليد.

التقليد يعني المحاكاة، وهو هنا إنشاء مصنف على غرار مصنف أصلي، بحيث يوهم المطلع عليه بأنه هو المصنف الأصلي، وهو ما يتحقق بالاعتداء على أي حق من حقوق المؤلف، ومن حيث المبدأ يجوز تشبيه التقليد بالاختلاس في السرقة،[4] وكل تقليد عبارة عن جنحة كما تنص على ذلك االمادة 2-l335 من قانون الملكية الفكرية الفرنسي، والمادة 151 من الأمر 05/03. وقد

---

[1] أشار المشرع الجزائري إلى مصطلح أصالة في قانون حماية حقوق المؤلف والحقوق المجاورة في أكثر من موضع، من ذلك م2/05، وم06. وفيما يخص البرمجيات فقد ثار جدل في فرنسا حول المعيار المتبع لتحديد مصطلح الأصالة، وعموما ظهر فريقان: فريق يعتمد على الطابع الشخصي، وهي النظرية التقليدية ومضمونها أن يخلع المبرمج على برنامجه شيئا من شخصيته تميزه عن غيره، غير أنه في هذا المجال يثور الشك حول ما إذا كان المبرمج عن طريق مجموعة من الاختيارات يعبر فعلا عن شخصيته، لذا فإن الفريق الآخر ينادي بتحوير مفهوم الأصالة ليصير ملائما للبرمجيات، عن طريق تقريب مفهوم الأصالة في البرمجيات إلى مفهومه في الاختراع، بحيث يتطلب نوعا من الجدة، وقد أخذت محكمة النقض الفرنسية بهذا الرأي في إحدى القضايا المطروحة أمامها ومما جاء في حيثيات الحكم: "إنه لا يجوز لمحاكم الموضوع استخلاص أصالة برنامج الحاسب الآلي من العمل الابتكاري الكامن في إنتاج ووضع البرنامج " مما يعني أن المحكمة قد أشارت إلى قرينة إضافية دالة على النشاط الابتكاري وهي الجدة، وهي هنا بمعنى أن يأتي واضع البرنامج بشيء جديد يختلف عن البرامج التي سبقته. انظر المرجع السابق، ص49 وما بعدها.

[2] المرجع نفسه، ص54.

[3] خالد حربي السعدي، جريمة إتلاف برامج ومعلومات الحاسب الآلي في التشريعين الكويتي والمقارن، دار النهضة العربية، القاهرة، مصر 2012، ص27.

[4] Christophe Caron, droit d'auteur et droits voisins, 3eme édition, lexis nexis, paris 2013, p459.

تطرق المشرع الجزائري في الأمر 05/03 إلى التقليد في المواد 151- 155، والملاحظ أنه اعتبر التعامل مع النسخ المقلدة ورفض دفع المكافأة المستحقة للمؤلف ضمن الأفعال المكونة لجنحة التقليد، وكان الأجدر اعتبارها جرائم ملحقة بجنحة التقليد.

وتتكون هذه الجريمة كغيرها من ركنين: مادي ومعنوي.

1 - الركن المادي لجريمة التقليد.

عادة ما يتكون الركن المادي من سلوك ونتيجة وعلاقة سببية بين السلوك والنتيجة. والسلوك الإجرامي في جريمة التقليد يتمثل في قيام الجاني بأحد أفعال الاعتداء على حق من حقوق المؤلف، وتتحقق النتيجة الإجرامية بمجرد الانتهاء من أي فعل منها، ولا بد من توافر العلاقة السببية بين السلوك الإجرامي والنتيجة، ويجتمع هنا السلوك الإجرامي والنتيجة والعلاقة السببية بينهما، حيث يكاد يتعاصر السلوك مع النتيجة ويتزاوجان داخل إطار العلاقة السببية بينهما.[1]

أ – محل السلوك الإجرامي.

محل السلوك أو النشاط الإجرامي في جريمة التقليد بصفة عامة هو المصنف المحمي، وقد نصت عليه المواد 3 وما بعدها من الأمر 05/03 سالف الذكر، وم140 من قانون حقوق الملكية الفكرية المصري، ومن بين المصنفات المحمية برامج الحاسب الآلي وقواعد البيانات سواء كانت مقروءة من الكمبيوتر أو من غيره.

يقصد بالمصنف الذي يستحق الحماية "كل عمل مبتكر أدبي أو فني أو عملي أيا كان نوعه أو طريقة التعبير عنه أو أهميته أو الغرض من تصنيفه"، ويقصد بالابتكار"الطابع الإبداعي الذي يسبغ الأصالة على المصنف"، أي أن المؤلف يكون قد أضاف من عبقريته إلى فكرة سابقة مما يجعل لها طابعا متميزا جديرا بالحماية، سواء تعلق ذلك بالفكرة أو المضمون، أو بطريقة العرض، أو بالتعبير عن الفكرة، أو بالتبويب.

[1] عبد القادر القهوجي، المرجع السابق، ص15.

وتنسحب برامج حماية الكمبيوتر على الأعمال التحضيرية، أي كل مراحل إعداد البرنامج، متى توافر شرط الأصالة بإحداها، وهذه المراحل هي: مرحلة تحليل المشكلة، مرحلة رسم خريطة الحل، مرحلة كتابة البرنامج، مرحلة ترجمة البرنامج،[1] وتستفيد من قانون حماية حق المؤلف كل أنواع البرامج: برامج مصدر، برامج هدف، برامج ترجمة، برامج تشغيل أو تنفيذ، برامج تطبيق، وأيا كانت الدعامة المثبت عليها البرنامج، وسواء تعلق الأمر بالنسخة الأصلية للبرنامج أو بنسخته الاحتياطية، كما تمتد الحماية إلى قواعد البيانات أو ما يماثلها، ولم يعرف المشرع قواعد البيانات، ولكن قرار وزير الثقافة المصري عرفها بأنها "تجميع متميز للبيانات يتوافر فيه عنصر الإبداع والابتكار أو الترتيب أو أي مجهود شخصي يستحق الحماية، وبأي لغة أو رمز، وبأي شكل من الأشكال، يكون مخزنا بواسطة حاسب، ويمكن استرجاعه بواسطته أيضا".[2] ويمكن تعريفها أيضا بأنها المعلومات أو المعطيات سواء قبل أو بعد معالجتها، وسواء كانت مخزنة في الحاسب أو غير مخزنة، شريطة أن يتوافر فيها الابتكار؛ والقول الفصل في توافر هذا الشرط أو عدمه يرجع إلى تقدير محكمة الموضوع التي لها أن تقدر ذلك سواء بالاستعانة بخبير أو دون ذلك.[3]

وحتى تستفيد برامج الحاسب الآلي وقواعد البيانات وما يماثلها بالحماية المقررة في قانون حقوق الملكية الفكرية، يجب أن تكون هذه المصنفات مما يخضع للحماية طبقا لأحكام القانون، فقد نصت م139 من قانون حقوق الملكية المصري على أنه: "تشمل الحماية المقررة لحقوق المؤلف والحقوق المجاورة لها المصريين والأجانب من الأشخاص الطبيعيين والاعتباريين الذين ينتمون إلى إحدى الدول الأعضاء في منظمة التجارة العالمية ومن في حكمهم، وتعتبر في حكم رعايا الدول الأعضاء: أ بالنسبة لحق المؤلف: 1 المؤلفون الذين تنشر مصنفاتهم لأول مرة إحدى الدول الأعضاء في المنظمة أو تنشر في إحدى الدول غير الأعضاء والدول الأعضاء في آن واحد، ويعتبر المصنف منشورا في آن واحد في عدة دول إذا ظهر في دولتين أو أكثر خلال ثلاثين يوما من تاريخ نشره لأول مرة..." وقد تطرق المشرع الجزائري إلى المصنفات المحمية في الباب الأول من الأمر 03-05 سالف الذكر في المواد من 03 إلى 11.

[1] القهوجي، المرجع السابق، ص19.

[2] المرجع نفسه، ص20.

[3] المرجع نفسه، ص21.

ب – السلوك الإجرامي.

يتمثل النشاط الإجرامي لجريمة التقليد في كل سلوك يتحقق به الاعتداء فعلا على حق من حقوق المؤلف دون إذن منه.

للمؤلف على مصنفه حق له مظهران: مظهر أدبي ومظهر مالي، فمن حقوق المؤلف الأدبية على مصنفه حق إتاحة المصنف للجمهور لأول مرة، حق احترام المؤلف ومصنفه، حق السحب أو الندم(التوبة)، أما أهم مظاهر الحق المالي للمؤلف فهي حقه في احتكار مؤلفه على الوجوه التي حددها القانون،[1] ويجرم المشرع الاعتداء على هذين المظهرين، مهما كانت صورهما، ومن أمثلة ذلك، الاعتداء على حق المؤلف في استغلال مصنفه، أو حقه في تقرير نشر المصنف، أو في تعيين طريقة هذا النشر، أو الاعتداء على حق المؤلف في نسبة المصنف إليه، أو في تعديل أو تحوير أو ترجمة أو سحب المصنف من التداول.

يكفي الاعتداء على أحد هذه الحقوق لقيام الجريمة، مهما كانت صورة الاعتداء أو جسامته، فالاعتداء على حق مؤلف برنامج الكمبيوتر في اختيار الوقت والطريقة التي يتم بها إذاعة أو نشر البرنامج، يتم عندما ينشر هذا البرنامج في وقت غير الذي يراه صاحب الحق ملائما، أو بطريقة غير التي يراها مناسبة له؛ وقد قضي أن انتهاك المتصرف إليه في البرنامج لشروط العقد الذي يربطه بمؤلف البرنامج، والتي بمقتضاها يحظر على الأول إعادة التصرف في الحقوق التي انتقلت إليه على البرنامج ولو عن طريق منح تراخيص من الباطن، يعد مساسا بالحق الأدبي للمؤلف.[2]

وبالنسبة للمصنف الجماعي، فإن الشخص الطبيعي أو المعنوي الذي يدير ويوجه نشاط المستخدمين في ابتكار البرنامج هو الذي يتمتع بحقوق المؤلف المالية والأدبية، وهو الذي يقرر تبعا لذلك وقت إذاعتها أو نشرها، ولا يعتبر ذلك اعتداء على حقوق المؤلفين الحقيقيين لمثل هذا النوع من البرامج لأن نصوص قانون حماية الملكية الفكرية تعطي لهذا الشخص وحده مباشرة حقوق المؤلف بصفة مطلقة، سواء كانت هذه الحقوق مادية أو أدبية.[3] ولكن يكون هذا الأمر في الفرض الذي

[1] حسام محمود لطفي، المرجع السابق، ص175.

[2] القهوجي، المرجع السابق، ص24.

[3] القهوجي، المرجع السابق، ص25.

يشترك فيه أكثر من فرد في إعداد البرنامج، أما إذا تولى إعداد البرنامج مجموعة بحيث يمكن فصل عمل المشتركين كل على حدة، فإن الشخص الطبيعي أو المعنوي الذي أدار العمل يكون هو المؤلف للمصنف في مجموعه، ولكن يثبت لكل مشترك ما دام عمله فيه أصالة، أن يتمتع بحق المؤلف على عمله فقط، وله تبعا لذلك أن يباشر جميع الحقوق المالية والأدبية على هذا العمل وحده، بشرط ألا ينافس المصنف الجماعي، فإذا اعتدى المستخدِم على حقوق الآخرين بإذاعة أو نشر عمل أحد المشتركين فقط أو إذاعة المصنف الجماعي يكون مرتكبا لجريمة التقليد.

وهذه النتيجة التي انتهينا إليها تطبيقا لنصوص قانون الملكية الفكرية المصري تعتبر مجحفة في مجال "صناعة البرامج" بالنسبة للمؤسسات التي تقوم بهذه الصناعة الهامة، نظرا للاستثمار الكبير الذي تبذله هذه المؤسسات للوصول إلى البرنامج المبتكر، ولهذا قرر المشرع الفرنسي في م45 من قانون حق المؤلف الصادر سنة 1985 منح الشخص المخدوم الحق في مباشرة الحقوق المادية والمعنوية للمؤلف، سواء كان البرنامج من إعداد مستخدم واحد أو عدة مستخدمين، وسواء أمكن فصل عمل كل منهم أو لم يمكن ذلك، شريطة أن تكون وظيفة المستخدم ابتكار البرامج.[1] وهذا ما نص عليه المشرع اللبناني صراحة في المادة الثانية من قانون حماية الملكية الأدبية والفنية.

وبخصوص المصنف المشترك، إذا اشترك في إعداد المصنف المبتكر عدة أشخاص، فإن الحق في تقرير إذاعة هذا المصنف يختلف بحسب ما إذا كان لا يمكن الفصل بين نصيب كل منهم أو كان يمكن ذلك، فإذا كان لا يمكن الفصل فإنه لا يجوز لأحدهم مباشرة حقوق المؤلف منفردا إلا بناء على اتفاق مكتوب بينهم، وإلا عد الفاعل مرتكبا جريمة التقليد، أما إذا أمكن الفصل بين نصيب كل شريك جاز لكل واحد منهم أن يقرر إذاعة أو نشر نصيبه منفردا دون أن يعد معتديا على حقوق غيره، بشرط ألا يضر ذلك باستغلال المصنف المشترك الذي يظل دائما من حق كل الشركاء مجتمعين.

[1] المرجع نفسه، ص26.

كما أن التشريعات المقارنة نصت على حق المؤلف الأدبي في منع تعديل المصنف تعديلا يعتبره المؤلف تشويها أو تحريفا له. ولا يعد التعديل في مجال الترجمة اعتداء إلا إذا أغفل المترجم الإشارة إلى مواطن الحذف أو التغيير أو أساء بعمله لسمعة المؤلف ومكانته.[1]

وللمؤلف الحق أيضا في نسبة المؤلف إليه (حق النسب أو حق الأبوة)، ولهذا تقوم جريمة التقليد عند نسبة البرنامج إلى شخص آخر غير مؤلفه أو إذا نسب أحد الشركاء البرنامج المشترك لنفسه فقط مستبعدا أسماء باقي الشركاء.

وقد تقع أفعال الاعتداء على الحق المالي للمؤلف في استغلال مصنفه بأي وجه من الوجوه، ومن أمثلة ذلك النسخ والاستعمال والترجمة (م02/151 من الأمر 05/03).

يقع الاعتداء فعلا على حق مؤلف البرنامج في نسخ برنامجه في الحالة التي يقوم فيها الجاني بنسخ المصنف دون إذن مؤلفه أو نسخ عدد من النسخ يفوق ما هو متفق عليه بينهما، ويستوي أن يكون المصنف ذا قيمة عالية أم لا، وفي حالة المصنف المشترك، إذا قام أحد مؤلفي البرنامج بنشره أو إعادة نشره دون موافقة الباقين أو دون إذن كتابي منهم عد مرتكبا لجريمة التقليد.

ويستوي أن يكون النسخ قد وقع كليا وهو ما يطلق عليه النسخ الحرفي الكامل، أو جزئيا وهو ما يطلق عليه النسخ الحرفي الجزئي، أو بطريق الاقتباس، أو التشويه عن طريق حذف أجزاء من المصنف.[2]

وتتوافر جريمة التقليد أيضا سواء تم نسخ المصنف باسم مؤلفه الحقيقي أو باسم شخص آخر يخلق لبسا في الأذهان حول مؤلفه الحقيقي، أو باسم الجاني نفسه، أو باسم خيالي.[3]

والعبرة في تقدير وجود التقليد هو بوجود الشبه لا بوجود الاختلاف.

ويدخل في حكم النسخ تثبيت البرامج على القرص الصلب للحاسب الآلي،[1] وقد يتخذ الاعتداء على حق المؤلف في استغلال برنامجه صورة الاستعمال، وذلك في كل حالة يتجاوز فيها من

[1] القهوجي، المرجع السابق، ص28.

[2] المرجع نفسه ص31.

[3] القهوجي، المرجع السابق، ص32.

يوجد بحيازته البرنامج حيازة مشروعة حدود الاتفاق بينه وبين المؤلف، ومثاله تثبيت البرنامج في جهاز آخر غير المرخص به، وهذا ما حكمت به المحكمة الإصلاحية لمدينة Cusset الفرنسية حين دانت رئيسها بتهمة التقليد لأنه قام بتثبيت برنامج مرخص له لحاسب واحد في باقي أجهزة المؤسسة.[2]

وتستثني المادة 44 من الأمر 05/03 والمادة171 مصري النسخ للاستعمال الشخصي، ويدخل فيه الاستعمال العائلي أو لغرض تعليمي، كما تُستثنى النسخ بغرض الحفظ، إذ يجوز لرب العمل أن يحتفظ بنسخة احتياطية من البرنامج يستخدمها في حالة تلف أو ضياع النسخة الأصلية (م52 من الأمر05/03 سالف الذكر).

وقد يتخذ الاعتداء على حق المؤلف في استغلال برنامجه صورة الاستعمال، وذلك في كل حالة يتجاوز فيها من يوجد بحيازته المصنف حيازة مشروعة حدود الاتفاق بينه وبين المؤلف.

وقد يتخذ الاعتداء صورة نقل برنامج الحاسوب إلى لغة أخرى دون ترخيص من المؤلف كأن يترجم من لغة المصدر إلى لغة الهدف، بل يمكن تصور الترجمة من لغة إجرائية إلى لغة إجرائية أخرى.

إذا نقل المؤلف حق استغلال مؤلفه إلى الغير فلا يجوز له التصرف فيه أخرى إلى شخص ثالث، فإذا تصرف فيه للمرة الثانية، فإن هذا التصرف الأخير يعتبر إخلالا بشروط التعاقد بين المؤلف والمتصرف إليه الأول. والسؤال الذي يفرض نفسه هنا: هل يعتبر المؤلف في هذه الحالة مرتكبا لجريمة التقليد؟ يرى جانب من الفقه عدم اعتبار ذلك، على أساس أن قانون حماية الملكية الفكرية إنما وضع لحماية المؤلف دون غيره، إلا أن جانبا فقهيا آخر له نظرة مغايرة ملخصها أن قانون الملكية الفكرية جاء لحماية الحقوق الأدبية والفنية لا الأشخاص، ومن ثم يتمتع بها المؤلف وغيره طالما أنه صاحب حق من حقوق التأليف.[3]

ويجب لقيام جريمة التقليد، أن يقع الاعتداء على حقوق المؤلف المالية خلال المدة التي يتمتع فيها المؤلف بالحماية، وهي حسب نوع المصنف، فإذا استغل البرنامج بأي صورة كانت بعد

---

[1] بن زيطة عبد الهادي، المرجع السابق، ص80.

[2] المرجع نفسه، ص81.

[3] القهوجي، المرجع السابق، ص35.

انتهاء المدة فلا تقوم جريمة التقليد لأن حقوق مؤلفي المصنفات المالية بعد انتهاء هذه المدة تسقط فيما يسمى الملك العام، ويصبح استغلال المصنف جائزا للجميع. غير أن الحق المعنوي أو الأدبي للمؤلف مؤبد وغير قابل للتنازل أو التقادم، وتنتقل بعض جوانبه إلى الورثة.[1]

ويشترط لتوافر النشاط الإجرامي في جريمة التقليد إلى جانب الاعتداء على حق من حقوق المؤلف، عدمُ وجود إذن كتابي من المؤلف أو خلفه، ويجب أن يكون هذا الإذن سابقا على أفعال الاعتداء أو معاصرا لها على الأقل، وبناء عليه فإن الإذن اللاحق لا يحول دون قيام الجريمة، ولا يؤثر على قيام الجريمة أيضا تسامح المجني عليه أو تنازله عن المطالبة بالتعويض عن الضرر الذي حاق به. وإذا كان المصنف محل الحماية مشتركا يجب أن يصدر الإذن الكتابي من قبل جميع الشركاء. وإذا تجاوز من صدرت له الموافقة مدى الحق الموافق عليه، أو تصرف بصدد حق آخر غير هذا الحق يعتبر مرتكبا لجريمة التقليد.

وقد اشترط كل من المشرع المصري واللبناني أن تكون الموافقة كتابية، والكتابة هنا شرط وجود لا شرط إثبات فقط، ومع ذلك فإن القضاء الفرنسي يتجه إلى اشتراط الكتابة في العلاقة بين المؤلف والناشر فقط، ويعلل ذلك أن المخاطر التي تنجم عن علاقة المؤلف بغير الناشر أقل بكثير من المخاطر التي تنجم بينه وبين الناشر.[2]

2 – الركن المعنوي لجريمة التقليد.

لم يصرح به المشرع في بعض القوانين المقارنة،[3] غير أن الفقه والقضاء يسلمان بضرورة توافره، وكذا القواعد العامة للقانون الجنائي.[4]

جريمة التقليد جريمة عمدية يلزم لقيامها توافر الركن المعنوي المتمثل في القصد الجنائي العام بعنصريه العلم والإرادة، علم بعناصر الجريمة وإرادة متجهة إلى السلوك الإجرامي ونتيجته.

---

[1] المرجع نفسه، ص36.

[2] المرجع نفسه، ص40.

[3] نص المشرع الجزائري صراحة على وجوب توافر القصد الجنائي من خلال نص م155 من الأمر 05/03: "كل من يرفض عمدا دفع المكافأة..."

[4] نصت م121-3 من قانون العقوبات الفرنسي على أن الجنايات والجنح تتطلب قصدا جنائيا.

ذهب اتجاه في الفقه إلى ضرورة توافر قصد خاص أيضا، يتمثل في سوء نية الجاني، غير أن القانون الفرنسي وكذا الجزائري والمصري لا يشترط مثل هذا الشرط، وعليه يكفي لقيام الركن المعنوي في جريمة التقليد توافر القصد الجنائي العام، بيد أن المشرع اللبناني نص في م86 من قانون حماية الملكية الأدبية والفنية على معاقبة الاعتداء أو محاولة الاعتداء على حق من حقوق المؤلف إذا تم ذلك بغية الربح، والذي يستفاد من النص هو تطلبه لقصد خاص هو إرادة تحقيق الربح، فإذا لم تكن نية الجاني تحقيق الربح انتفى الركن المعنوي، وبالتالي لا تقوم الجريمة.

لكن المتفق عليه في الفقه والقضاء بفرنسا أن القصد الجنائي في جريمة التقليد مفترض،[1] بمعنى أن تحقق إحدى صور السلوك الإجرامي يعد قرينة كافية للقول بتوافر القصد الجنائي، أي أن حسن النية لا يفترض في هذه الجريمة، بيد أن هذه القرينة بسيطة تقبل إثبات عكسها، ولكن من الصعب عمليا أن يستطيع المتهم إثبات حسن نيته، وتقدير ذلك كله لمحكمة الموضوع دون رقابة عليها من محكمة النقض طالما كان ذلك مبنيا على أسباب معقولة.[2]

قانون أول أوت 2006 الفرنسي أوجد جنحة خاصة نصت عليها م 1-2-335l من قانون الملكية الفكرية الفرنسي تعاقب من وضع **عمدا** في متناول الجمهور برنامجا يسهل التداول غير المرخص به للمصنفات، وهذه المادة تنسحب أيضا على الملفات المتبادلة عبر الإنترنت، والسؤال المطروح: هل تطبق على هذه الجنحة أيضا قاعدة النية السيئة أي افتراض القصد الجنائي؟ والسؤال ذاته يطرح بشأن الجرائم المتعلقة بتدابير الأمن التقنية التي تتمتع بها البرامج وبالمعلومات حول المصنفات الواردة في المادتين: 1-3-335l و2-3-335l من قانون الملكية الفكرية الفرنسي.[3]

3- العقوبات المقررة لجنحة التقليد.

عاقبت القوانين المقارنة أفعال التقليد بعقوبات أصلية وأخرى تكميلية.

---

[1] Delphine Galan, la protection de la création olfactive par le droit de la propriété intellectuelle, thèse Pour obtenir le grade de docteur de l'université d'AVIGNON et des pays de VAUCLUSE, Discipline : Droit privé, faculté de droit, france2008, p472.

[2] القهوجي، المرجع السابق، ص42.

[3] Christophe Caron, op.cit. p477.

أ- العقوبات الأصلية:

نصت م153 من الأمر 05/03 على عقوبة جنحة التقليد وهي الحبس من ستة أشهر إلى ثلاث سنوات والغرامة من ½ مليون د ج إلى مليون دينار، والملاحظ أن المشرع قد جمع عقوبة الغرامة مع العقوبة السالبة للحرية ولم يدع للقاضي خيار توقيع إحداهما فقط أو الجمع بينهما. وعاقبت م154 من الأمر السابق كل من يشارك بعمله أو بالوسائل التي يحوزها للمساس بحقوق المؤلف. وفي حالة العود تضاعف العقوبات.

أما المشرع الفرنسي فقد نص في م 2-l335 من قانون الملكية الفكرية على عقوبة الحبس ومدتها القصوى تصل إلى ثلاث سنوات، ووضع ظرفا مشددا هو ارتكاب الجنحة ضمن عصابة منظمة حينها تصل العقوبة السالبة للحرية إلى خمس سنوات حبسا، وفي حالة العود تضاعف العقوبة، أما العقوبات المالية فيجوز أن تصل 300.000 يورو، بل 500.000 يورو في حال ارتكابها ضمن عصابة منظمة.

يرى جانب من الفقه الفرنسي أنه حتى في حالة إقرار المشرع الفرنسي لعقوبات سالبة للحرية فإن الغرامة المالية هي الأكثر ملاءمة ونفعا في مثل هذا النوع من الجرائم، إذ عادة ما يلجأ إلى التقليد لأسباب مالية، كتجنب اقتناء النسخة الأصلية باهظة الثمن نسبيا، أو لبيع النسخ المقلدة وتحقيق ربح، لذا فإن الأجدر في عملية الردع هنا تغليظ عقوبة الغرامة جزاء وفاقا، لكي يعلم المقلدون أنهم سيخسرون كثيرا إن أقدموا على التقليد في حالة القبض عليهم من طرف رجال إنفاذ القانون.[1]

وعليه ندعو المشرع الجزائري إلى مراجعات لقيمة الغرامة، ورفعها دوريا، لأن العقوبات المالية أكثر تحقيقا للردع بالنسبة لهذا النوع من الجرائم. والملاحظ أن المشرع الفرنسي عاقب أيضا صراحة الشخص المعنوي المرتكب لجنحة التقليد.

ب- العقوبات التكميلية:

نص المشرع الجزائري في م2/156 من الأمر 05/03 على عقوبة الغلق المؤقت لمدة لا تتجاوز ستة أشهر، ونص في م157 من الأمر السابق على مصادرة المبالغ الناتجة عن الاستغلال غير

[1] Guillaume Blanc- Jouvant, droit de la propriété intellectuelle, Vuibert, Paris 2011,p138.

الشرعي للبرنامج، ومصادرة وإتلاف كل عتاد أنشئ لمباشرة النشاط غير المشروع، وكل النسخ المقلدة، كما نص في م158 من الأمر السابق على جواز نشر أحكام الإدانة كاملة أو مجزأة في الصحف التي يتم تعيينها، وتعليقها في الأماكن التي تحددها المحكمة، من ضمن ذلك باب منزل المحكوم عليه، وكل هذا على نفقته.

أما المشرع الفرنسي فقد نص علاوة على العقوبات التكميلية السابقة على عقوبة الحرمان من الولوج إلى الإنترنت لمدة قد تصل إلى سنة واحدة، بنص م 7-335l من قانون الملكية الفكرية الفرنسي التي استحدثت بقانون 28 أكتوبر 2009 المتعلق بالحماية الجزائية للملكية الفكرية عبر الإنترنت.[1]

ثانيا: الجرائم الملحقة بجرائم التقليد.

أورد كل من المشرع الفرنسي والمشرع المصري جرائم أخرى في قانون الملكية الفكرية، اصطلح عليها الجرائم الملحقة بجنحة التقليد أو الجرائم الشبيهة بها.

1- الجرائم الملحقة بالتقليد في القانون الفرنسي

أورد المشرع الفرنسي جريمتين شبيهتين بالتقليد هما: المساس بحماية تدابير تقنية الحماية والمعلومات[2] وواجبات ومسؤولية المنخرطين عبر شبكة الإنترنت.

أ- جريمة المساس بحماية تدابير تقنية الحماية والمعلومات

تناولت هذه الجريمة م1-3-335l فيما يخص التدابير التقنية، وم2-3-335l فيما يخص المعلومات، وهذه الجريمة عمدية تتطلب قيام القصد الجنائي العام، وتهدف إلى حماية التدابير التقنية الموضوعة لبرنامج ما وكذا المعلومات الرقمية حول البرنامج، وتعاقب المادتان من يصنع أو يستورد معدات أو برامج من شأنها المساس بالتدابير التقنية، كما تعاقب من يبيع أو يؤجر أو يساعد على المساس بالتدابير التقنية أو المعلومات الرقمية التي عدل أو حذف عمدا أحد عناصرها.[3]

---

[1] Christophe Caron, op. cit, p525.
[2] La protection des mesures techniques de protection et des informations.
[3] Christophe Caron, op. cit, p529.

ب- جريمة الإخلال بواجبات ومسؤولية المنخرطين عبر شبكة الإنترنت.

الهدف من إيجاد هذه الجريمة هو دفع المنخرطين في الإنترنت إلى مزيد من الحرص، بمعنى أن يكونوا أكثر يقظة فيما يخص من يرتكب أو يتعامل مع مصنفات مقلدة انطلاقا من حاسبهم الآلي وهنا تبرز فكرة المسؤولية عن فعل الغير، وكذلك حث المنخرطين على المسارعة في طلب الحماية التقنية لحاسباتهم الآلية.

تطرقت إلى هذه الجريمة م3-l336 من قانون الملكية الفكرية، وعاقبت على إخلال المنخرط بواجب الحرص بحرمانه المؤقت من الولوج إلى الإنترنت، مع استمرار دفع ثمن الاشتراك، وعدم إمكانية التعامل مع مزود خدمة إنترنت آخر إلا بدفع غرامة قدرها 3750 يورو.[1]

2- الجرائم الملحقة بالتقليد في القانون المصري

تطرق المشرع المصري في قانون حماية حقوق الملكية الفكرية إلى جريمة نشر مصنف أو التعامل فيه، وجريمة تقليد المصنفات أو التعامل فيها وذلك في م181 من أولا إلى سادسا.

أ- جريمة نشر مصنف أو التعامل فيه

المتأمل في الأفعال التي تتكون منها هذه الجريمة يلاحظ أنها تدخل في الأفعال التي تقع بها جريمة التقليد، ولذلك يكون النص على الأفعال السابقة تكرار لما سبق، أو تطبيقا من تطبيقات صور الاعتداء على حق من حقوق المؤلف الأدبية والمالية، وكان يفضل عدم النص عليها استقلالا كما فعل المشرع اللبناني.

ب- جريمة تقليد المصنفات أو التعامل فيها

نصت م2/181 مصري على معاقبة كل من ارتكب فعل تقليد مصنف أو بيعه أو عرضه للبيع أو للتداول أو الإيجار مع العلم بتقليده.

وفعل التقليد المنصوص عليه في هذه المادة لا يختلف عن ما رأيناه فيما سبق، ولذلك فإنه من الأجدر لو استغنت هذه المادة عن لفظ التقليد واكتفت بالتعامل في المصنف المقلد، الذي

[1] I bid, p536.

يشمل البيع والعرض للبيع والتداول والإيجار، ويضيف المشرع اللبناني المودع عنده مصنفا مقلدا، ويكفي لتوافر السلوك الإجرامي مجرد الإيداع، أي وجود المصنف المقلد لدى المودع لديه، ويجرم المشرع اللبناني مجرد تقليد إمضاء المؤلف أو إشارته بقصد خداع المشتري وحمله على إبرام الصفقة، أو بقصد جني ربح غير مشروع حتى ولو لم يوجد مشتر يقصد خداعه، وهو ما يدخل في نطاق التقليد بصفة عامة.

والملاحظ أن المشرع المصري لم يجرم أفعال التصدير أو الشحن للبرامج المقلدة، رغم خطورتها، ولكنه جرم هذه الأفعال بالنسبة للمصنف المنشور في الخارج والذي تم تقليده في مصر (م3/181 مصري) مما يعني أن المشرع المصري حمى المؤلف الأجنبي أكثر من المؤلف المصري.[1]

والركن المعنوي في هذه الجريمة هو القصد العام الذي يتوافر في كل حالة يعلم فيها الجاني أن ما يبيعه أو يعرضه للبيع أو يتداول فيه أو يؤجره أو يودَع عنده هو مصنف مقلد، وأن تتجه إرادته إلى ذلك، والقصد الجنائي هنا مفترض أيضا بحيث يعتبر تحقق الركن المادي قرينة بسيطة على توافره، وعلى الجاني إثبات حسن نيته، ولمحكمة الموضوع سلطة تقدير واسعة دون رقابة عليها من محكمة النقض.[2]

بالإضافة إلى هاتين الجريمتين نص المشرع المصري على جريمة الاعتداء على الحماية الفنية التي يستخدمها المؤلف (م6،5/181 مصري) كما فعل المشرع الفرنسي.

وبالنسبة للعقوبات فقد نص المشرع المصري على العقوبات ذاتها بالنسبة لكل الجرائم، وهذه العقوبات أصلية وتكميلية، فالعقوبات الأصلية عبارة عن الحبس والغرامة، وتشدد إذا وجد ظرفان مشددان هما تعدد المصنفات محل الجريمة والعود، أما العقوبات التكميلية فهي عبارة عن المصادرة، الغلق، ونشر ملخص الحكم.

[1] القهوجي، المرجع السابق، ص47.

[2] القهوجي، المرجع السابق، ص48.

المطلب الثاني: حماية أسماء النطاق على شبكة الانترنت.

موضوع أسماء النطاق حديث نسبيا، فرضته التغيرات الكبيرة الحاصلة في عالم الانترنت، ولا يزال يثير الكثير من الإشكاليات القانونية خاصة فيما يتعلق بطبيعته القانونية ومدى ارتباطه بغيره من المصطلحات القانونية المشابهة له، وخاصة العلامة التجارية.

يعالج هذا المطلب من خلال التطرق إلى ماهية أسماء النطاق (الفرع الأول) وإلى النزاعات بين أسماء النطاق والمواضيع القانونية الأخرى خاصة العلامة التجارية (الفرع الثاني).

الفرع الأول: ماهية أسماء النطاق.

يحاول هذا الفرع معالجة أهم النطاق المتعلقة بماهية أسماء النطاق، فيتطرق أولا إلى مفهوم أسماء النطاق، الطبيعة القانونية لهذه الأسماء، ثم أنواع أسماء النطاق.

أولا: مفهوم أسماء النطاق.

أثار تعريف اسم النطاق جدلا كبيرا في آراء الفقه وأحكام القضاء، فمن التعريفات من تستند إلى الطبيعة الفنية لاسم النطاق، ومنها من تستند إلى تكوين اسم النطاق، ومنها من تستند إلى وظيفة الاسم.

واسم النطاق يطلق عليه أيضا "اسم الدومين"، "Nom de domaine" أو العنوان الالكتروني، أو اسم المجال، أو اسم حقل الانترنت.[1]

ركزت بعض الآراء على الطبيعة الفنية للعنوان الالكتروني فوصفته بأنه "مجرد تحويل أو نقل مجموعة من الأرقام في صورة حروف تشكل مصطلحا تتماشى مع اسم المشروع أو المنظمة"، أو بأنه "ترجمة لأرقام تتم عن طريق حروف معينة تسمح بتداول المعلومات عبر شبكة الانترنت"، فمستخدم الانترنت كان يكتب مجموعة من الأرقام للوصول إلى الموقع الذي يريده، ونظرا لصعوبة الأمر

[1] يراجع: د. خالد ممدوح إبراهيم،
- الجرائم المعلوماتية، دار الفكر الجامعي، الأزريطة، الإسكندرية، مصر 2009، ص370 وما بعدها.
- حقوق الملكية الفكرية، الدار الجامعية، الإسكندرية، مصر 2010، ص623 وما بعدها.
- أمين أعزان، المرجع السابق، ص366 وما بعدها.

استبدلت الأرقام بحروف سهلة للاستعمال، على أن تترجم هذه الحروف إلى أرقام عند وصولها إلى الخادم "Serveur" فيتعرف على الموقع المطلوب.[1]

أما جانب آخر من الفقه فعرف العنوان الالكتروني مستندا إلى مكوني هذا العنوان، وهما الجزء الثابت والجزء المتغير، فالجزء الثابت يتكون دوما من المقطع:(http://www)، ويشير إلى البروتوكول المستخدم، ويبين أن البروتوكول متواجد على شبكة الاتصالات العالمية، ويثبت هذا الجزء إلى جميع المشروعات والشركات والأشخاص الذين يمتلكون مواقع على الشبكة، أما الجزء المتغير فهو الذي يلي الجزء الثابت، وهو الذي يميز المشروع عن غيره من المشروعات، وهو الذي يطلق عليه العنوان الإلكتروني، وينقسم إلى نوعين، الأول هو العنوان الإلكتروني من الدرجة الأولى (TLD) ويمثله المقطع (com.) أو (org.) أو (net.) أو العناوين الإلكترونية التي تنتهي بحرفين من حروف الدول والمسماة العناوين الإلكترونية الوطنية مثل (dz.)، والثاني هو العنوان الإلكتروني من الدرجة الثانية (SLD)، ويمثله الحروف الأولى من اسم المشروع أو المنظمة أو حروف كل الاسم. ويلاحظ على هذا النوع من التعريفات أنه يصف تكوين العنوان الإلكتروني ويحدد علاقته بالموقع باعتباره جزءا منه، ولا يحاول وضع تعريف عام له.[2]

رأى جانب آخر من الفقه والقضاء أن يعرف العنوان الالكتروني بالنظر إلى وظيفته، ومن بين التعاريف التي صيغت: "إن العنوان الإلكتروني بديل عن العنوان البريدي، محدد للتعرف على شخص بعينه عبر شبكة المعلومات"، "إن العنوان الإلكتروني ليس سوى وسيلة تمكن مستخدمي الانترنت من الوصول إلى المواقع عبر الشبكة"، فهو استنادا إلى هذا الرأي، ليس إلا مجرد عنوان للهيئات والمنظمات والمشروعات والأشخاص، يمكن الوصول إليها عن طريقه، أو هو مجرد وسيلة للولوج إلى شبكة المعلومات، إلى عنوان موقع بعينه.[3]

وبهذا المعنى عرفت محكمة استئناف باريس العنوان التجاري الإلكتروني في حكم لها صادر عام 2000، حيث أشارت أنه وسيلة اتصال بالمشروعات والمنظمات الدولية والهيئات المختلفة

[1] شريف محمد غنام، المرجع السابق، ص10-11.

[2] شريف محمد غنام، المرجع السابق، ص13.

[3] د. هدى حامد قشقوش، الحماية الجنائية للتجارة الإلكترونية عبر الانترنت، دار النهضة العربية، القاهرة 2000، ص78.

على شبكة الانترنت، مؤكدة أنه مجرد عنوان افتراضي "simple adresse virtuelle" يحدد مواقع المشروعات على شبكة الانترنت.[1]

ويمكن القول بأن هذا النوع من التعريفات يعتمد على الوظيفة التي يؤديها العنوان الالكتروني، كونه مجرد عنوان للمشروعات على شبكة الانترنت، وهو عنوان افتراضي، يعادل عنوان المشروعات على أرض الواقع. ولعل أصحاب هذا الرأي هم الأكثر توفيقا في تعريف العنوان الإلكتروني.[2]

وقد عرف قانون التجارة الإلكترونية المصري اسم الدومين بأنه "عنوان متفرد للمواقع الموجودة على شبكة الانترنت، تسمح بتحديد الموقع وتميزه عن غيره"، وهو بذلك يحظى بأهمية كبيرة، حيث يعبر عن مؤسسة اقتصادية أو تجارية، مما يدعو لحمايته القانونية ووضع ضوابط لتسجيله.[3]

ثانيا: الطبيعة القانونية لأسماء النطاق.

أثار موضوع الطبيعة القانونية لأسماء النطاق (العناوين الالكترونية) جدلا واسعا بين الفقهاء خاصة في فرنسا، إلا أنه يمكن تصنيفها إلى اتجاهين: اتجاه يرى أن العنوان الإلكتروني لا ينتمي إلى عناصر الملكية الصناعية، واتجاه آخر يرى عكس ذلك، فبخصوص الاتجاه الأول انقسم بدوره إلى ثلاثة آراء؛ يرى أولها أن اسم النطاق موطن افتراضي للأشخاص على شبكة الانترنت،[4] ويرى ثانيها أن اسم النطاق يتطابق مع رقم الدخول في خدمة المينتال، مما يستتبع ذلك تطبيق الأحكام نفسها المطبقة على رقم الدخول بالنسبة لاسم النطاق،أما الرأي الثالث فيعتبر أن اسم النطاق فكرة قانونية مستقلة بذاتها مستندا إلى بعض أحكام القضاء الفرنسي.[5]

---

[1] شريف محمد غنام، المرجع السابق، ص14.

[2] المرجع نفسه، ص15.

[3] كوثر مازوني، الشبكة الرقمية وعلاقتها بالملكية الفكرية، دار هومة، الجزائر 2008، ص187.

[4] ومن بين القضايا التي أثيرت أمام القضاء الفرنسي بهذا الشأن قضية أحد طلبة المدرسة العليا للاتصالات الذي قام بإنشاء موقع باسمه عن طريق شبكة المدرسة، وسجل عليه أغنيات حديثة لمطرب فرنسي، مما جعل وكيل هذا المطرب والذي يحتكر نشر هذه الأغنيات يتقدم بدعوى ضد الطالب والمدرسة، لانتهاك حقوق المؤلف والحقوق المجاورة، وقد احتج الطالب والمدرسة بحجج كثيرة منها أن الموقع الذي يملكه الطالب يعد موقعا خاصا به لا موطنا عاما موجها إلى الجمهور، لا يجوز الإطلاع عليه تحت طائلة الاعتداء على حرمة الحياة الخاصة. وقد رفضت المحكمة هذه الحجج إذ لا يجوز اعتبار اسم النطاق موطنا خاصا لشخص، فبمجرد تصميمه فهو موجه إلى كل مستخدمي الانترنت، ويجوز للكل الإطلاع عليه.يراجع: أمين أعزان، المرجع السابق، ص382.

[5] أمين أعزان، المرجع السابق،ص ص384- 385.

والراجح هو الاتجاه الثاني الذي يقضي بأن العنوان الالكتروني أو اسم النطاق يندرج ضمن عناصر الملكية الصناعية، فهو مثل العلامة التجارية والاسم والعنوان التجاري، ومن ثم يستفيد من التنظيم القانوني لهذه العناصر. ويعتبر العنوان الالكتروني بهذا الوصف أحد العناصر المعنوية للمحل التجاري، إذ يشكل الدعامة التي تقوم عليها السمعة التجارية والاتصال بالعملاء. والسؤال هل اسم النطاق عنصر جديد من عناصر الملكية الصناعية؟ أم هو متطابق مع أحد عناصرها الموجودة؟ هناك بعض الاختلافات البسيطة الموجودة بين العنوان الالكتروني وبين عناصر الملكية الصناعية بصفة عامة، إلا أن ذلك مرده إلى أن العنوان الإلكتروني يقوم بدور عناصر الملكية عبر شبكة الانترنت، ومن هذه الاختلافات أن حق مسجل العنوان الالكتروني هو حق مطلق – بخلاف حق مالك العلامة التجارية أو الاسم أو العنوان التجاري – إذ بمجرد تسجيل هذا العنوان يمتنع على الغير تسجيل هذا العنوان مرة أخرى حتى ولو كان لتمييز منتجات أخرى أو مشروعات أخرى تتعامل في أنشطة مغايرة.[1] ذلك أن العنوان الإلكتروني قد تعاظم دوره على شبكة الانترنت، فلم يعد مجرد وسيلة للإعلان عن المشروعات عبر هذه الشبكة، بل تعدى ذلك ليصبح المميز لهذه المشروعات والمحدد لهويتها، بسبب القاعدة التي تحكم تسجيل العنوان الإلكتروني "قاعدة الأسبقية في التسجيل".[2]

ومن خلال ما سبق يميل الفقه إلى القول بأن اسم النطاق هو أحد العناصر الجديدة للملكية الصناعية، بحاجة إلى تدخل تشريعي سريع يحكمه وينظمه ويبرز خصوصياته.[3]

ثالثا: أنواع أسماء النطاق.

يجب التنويه أولا أن أسماء النطاق تخضع لشروط تقنية، من أهمها أن لا يتجاوز طولها ثلاثة وستين مكونا، وأن لا يقل عن مكونين اثنين بالنسبة ل: ".org" ".net" ".com" وعن ثلاثة مكونات بالنسبة ل: ".fr"، كما لا يجوز أن يبدأ اسم النطاق أو ينتهي ب: "-" كما لا يجوز استخدام المكون فراغ "espace" في الاسم.[4]

---

[1] شريف محمد غنام، المرجع السابق، ص65.

[2] المرجع نفسه، ص252.

[3] خليفي مريم، الرهانات القانونية للتجارة الإلكترونية، أطروحة لنيل شهادة الدكتوراه في القانون الخاص، كلية الحقوق والعلوم السياسية، جامعة أبي بكر بلقايد، تلمسان، 2012/2011، ص296.

[4] Romain v.gola. droit du commerce électronique.Galino lextenso éditions. Paris. France 2013. P40.

نظرا للتزايد الهائل لأسماء النطاق على شبكة الانترنت، فقد تم تقسيمها إلى نوعين: نطاقات من المستوى الأول أو العالي ونطاقات من المستوى الثاني.[1]

1: النطاقات من المستوى الأول

هي التي توجد إلى اليمين من آخر نقطة من اسم النطاق، وتنقسم هذه النطاقات بدورها إلى ثلاثة أنواع: النطاقات النوعية، الجغرافية، والجهوية.[2]

تشكل اللواحق النوعية "extensions génériques" 80% من مجموع أسماء النطاق في العالم، وتعتبر اللاحقة ".com" الخاصة بالمؤسسات التجارية الأكثر أهمية بالنسبة لهذا النوع من النطاقات[3]، وهذه اللواحق هي: .int .mil .apra .gov .edu .net .org .com. وأضافت منظمة الأيكان التي تضطلع بمهمة تنسيق وتسجيل أسماء النطاق على المستوى العالمي سنة 2000 لواحق عامة أخرى وهي: .pro .name .museum .info .coop .biz .aero. وأضافت الأيكان سنة 2005 لواحق أخرى هي: .mobi .tel .travel .jobs .cat.

أما أسماء النطاق الجغرافية أو الإقليمية، فهي أسماء تخصص كل لاحقة منها لدولة فمثلا: dz. للجزائر وfr لفرنسا وeg لمصر.وكل دولة حرة في اختيار الجهة التي تمنح هذه المواقع، ففي الجزائر مثلا فإن الهيئة المختصة في منح اسم الموقع على شكل dz. هي مركز البحث في الإعلام العلمي والتقني " cerist" وذلك منذ جوان 1999[4]، وفي لبنان أنيطت المهمة إلى مكتب خاص تابع للجامعة الأمريكية في بيروت،[5] أما في فرنسا فإن المركز الفرنسي لمعلومات شبكة الانترنت "afnic "هو المسؤول عن الأسماء المرتبطة ب fr. وتضع هذه الهيئات الشروط اللازمة لمنح وتسجيل أسماء النطاق، وتزود مجتمع الانترنت بعناوين بروتوكول الانترنت التي تلزم للدخول إلى الشبكة العنكبوتية، وهناك مؤسسات عالمية متخصصة في الجانب التقني تتولى التنسيق بين عمل هذه الهيئات، وهي "ripe" في

[1] د. فاتن حسين حوى، المواقع الإلكترونية وحقوق الملكية الفكرية، دار الثقافة، عمان الأردن 2010، ص55.

[2] Romain v.gola. op cit. p39.

[3] Romain v.gola. op cit. p39.

[4] كوثر مازوني، المرجع السابق، ص198.

[5] د. فاتن حسين حوى، المرجع السابق، ص58.

منطقة أوربا، وشمال إفريقيا والشرق الأوسط، ومؤسسة"arin " في الأمريكيتين، ومؤسسة "apnic " لباقي إفريقيا وآسيا.[1]

أما الأسماء الجهوية فهي متعلقة باللاحقة "eu." التي تخص القارة الأوربية، ودخلت حيز التنفيذ سنة 2002، والهدف منها تقوية الهياكل القاعدية للانترنت في أوربا، وتدعيم التجارة الإلكترونية.[2]

والقاعدة المطبقة في تسجيل اسم الموقع هي: من يصل أولا يخدم أولا لذلك يرفض تسجيل اسم نطاق تم تسجيله من قبل بغض النظر عمن قام بتسجيله.[3]

2: النطاقات من المستوى الثاني

تتكون من الجزء الذي يقع على يسار آخر نقطة في اسم النطاق، حيث يجوز للهيئة المسؤولة عن تسجيل وإدارة النطاقات من المستوى العالي توزيع الخدمة على مستويات أدنى، ومن أمثلة ذلك: havard.edu، وcom.dz وorg.dz حيث يعتبر كل من edu وdz من المستوى الأول، وcom، org ،havard من المستوى الثاني.[4]

الفرع الثاني:النزاعات القانونية لأسماء النطاق

تثير أسماء النطاق الكثير من الإشكالات القانونية، خاصة مع العلامات التجارية، ورغم أن "الأيكان" قد وضعت قواعد موحدة لتسوية النزاعات المتعلقة بأسماء النطاق بطريقة ودية تعرف ب UDRP، إلا أن ذلك لا يمنع الخصوم من اتباع طريق القضاء. ولعل أبرز ما يثير الانتباه في هذا الشأن هو ما اصطلح عليه بعض الفقه: القرصنة الالكترونية.

أولا: التنازع بين اسم النطاق والعلامة التجارية.

يطلق بعض الفقه على التنازع بين اسم النطاق والعلامة التجارية مصطلح القرصنة الإلكترونية، وهي أن يقوم شخص أو مشروع لا يمتلك أي حق على علامة تجارية بتسجيل هذه

[1] د.عدنان إبراهيم سرحان، أسماء النطاق على الشبكة العالمية للمعلوماتية، مجلة الشريعة والقانون، العدد25، يناير 2006، ص305.

[2] Romain v.gola. op cit. p55.

[3] كوثر مازوني، المرجع السابق، ص199.

[4] المرجع نفسه، ص199.

العلامة في صورة اسم نطاق على شبكة الانترنت، بقصد الإضرار بمالك هذه العلامة، أو بقصد بيع العنوان الإلكتروني إلى هذا المالك بثمن مغال فيه، أو بيعه لأحد منافسيه.[1]

ونميز هنا بين عدة حالات: هي تسجيل اسم نطاق متطابق مع علامة تجارية مشهورة، وهو من أكثر الاعتداءات شيوعا، ومن الأمثلة الحية عن ذلك قيام المدعو موريس بتسجيل العلامة التجارية marlboro كاسم نطاق، مما حذا بالشركة أن تطلب من "الويبو" أن تقوم بتحويل اسم النطاق لصالحها،[2] ومن الحالات أيضا تسجيل اسم نطاق متشابه مع علامة تجارية مسجلة أو يحتوي عليها، وهنا يقوم من يسجل اسم النطاق بإدخال تعديل بسيط على إحدى حروف العلامة التجارية أو الطريقة التي تكتب بها ومن أمثلة ذلك إقدام شخص على تسجيل اسم نطاق كالآتي: www.ammazon.com المتشابه مع العلامة التجارية المملوكة لشركة amazon، حيث أضاف حرفا واحدا وهو m، ومن الحالات أيضا تسجيل اسم نطاق يحتوي على علامة تجارية غير مسجلة ولكنها ذات شهرة، ومن أمثلة ذلك قيام أحدهم بتسجيل لاسم نطاق يتكون من اسم الممثلة المشهورة جوليا روبرت، وقد حكم بإعادة اسم النطاق ولو لم يكن مسجلا كعلامة تجارية بالنظر للشهرة التي تحظى بها الممثلة الأمريكية.[3]

وقد تنبه القضاء في أوربا و الو. م. أ منذ عام 1996 إلى خطورة هذا العمل، فأصدر العديد من الأحكام التي تدينه بكل صوره، مستندا في أحكامه إلى العديد من الأسس القانونية منها قواعد المنافسة غير المشروعة، قواعد أحكام قانون العلامات التجارية وقانون حماية الملكية الفكرية، والقواعد التي تتضمنها القوانين الخاصة التي سنت خصيصا للتصدي لهذه الظاهرة.

من الأحكام القضائية التي صدرت بإدانة القرصنة الإلكترونية، الحكم الصادر من إحدى المحاكم الابتدائية بفرنسا عام 2000 والذي جاء فيه "إن البيع بالمزاد العلني لعناوين إلكترونية مقلدة لعلامات تجارية مشهورة يشكل عملا من أعمال القرصنة توجب مسؤولية من اشترك فيها".[4]

---

[1] شريف محمد غنام، المرجع السابق، ص102.

[2] د فاتن حسين حوى، المرجع السابق، ص177.

[3] د فاتن حسين حوى، المرجع السابق، ص179- 180.

[4] شريف محمد غنام، المرجع السابق، ص104.

وترتكز معظم الأحكام الصادرة بإدانة القرصنة الالكترونية على سوء نية من يقوم بها، عند تسجيله للعناوين الإلكترونية أو عند استخدامه لها، ويستشف القضاء سوء نية مسجل العنوان الإلكتروني من عدة مؤشرات منها: بيع العنوان الإلكتروني بعد تسجيله إلى المالك الشرعي للعلامة التجارية أو لأحد منافسيه بأثمان باهظة، حتى أن هناك العديد من المواقع عبر شبكة الانترنت مختصة ببيع العناوين الإلكترونية، بحيث يكتب العنوان والثمن المطلوب لبيعه، ويعتبر القضاء مجرد عرض العنوان للبيع على شبكة الانترنت قرصنة يسأل من يقوم بها حتى ولو لم يتم البيع فعلا، فمجرد العرض للبيع يكشف عن سوء نية القرصان في الاستفادة من المتاجرة في العنوان الإلكتروني. كما تستشف سوء النية من ظروف الواقعة ذاتها، وتستشف سوء النية أيضا إذا كان الهدف من تسجيل العنوان الإلكتروني هو الإضرار بمالك العلامة التجارية، بمنعه من تسجيل عناوين تمثل علامته على شبكة الانترنت.

ومن أهم العوامل المشجعة على القرصنة الإلكترونية، مبدأ الأسبقية في التسجيل الذي يسمح لأي شخص أو مشروع، بتسجيل عنوان إلكتروني على شبكة الانترنت ما دام أن العنوان لم يسبق تسجيله من قبل. ولا تشترط الجهات المختصة عن تسجيل العناوين الإلكترونية العامة أي شرط آخر للحصول عليه.

كما أن شهرة العلامة التجارية تشجع القرصان على الاعتداء عليها على شبكة الانترنت، بقصد استفزاز مالكها وحمله على شرائها بأموال مبالغ فيها، أو من أجل الإساءة إلى مالكيها والإضرار بهم.

والملاحظ أن القرصنة الالكترونية تزداد بالنسبة للعناوين الالكترونية العامة لشهرتها الواسعة بين الجمهور، ولقلة الرقابة السابقة عليها، على خلاف العناوين الإلكترونية الوطنية، التي تتطلب –كما هو الحال في فرنسا مثلا– أن يقدم المسجل شهادة تفيد ملكيته للعلامة التي يرغب في تسجيل عنوان إلكتروني يمثلها.[1]

[1] شريف محمد غنام، المرجع السابق، ص112.

يفرق القضاء في حمايته للعلامات التجارية بين العلامات المسجلة قبل تسجيل العنوان الإلكتروني، وتلك المسجلة بعد تسجيل العنوان الإلكتروني؛ فبالنسبة للعلامات التجارية المسجلة سابقا، فإن قوانين حماية الملكية الفكرية تعاقب كل من يزور علامة تجارية تم تسجيلها طبقا للقانون، أو قلدها بطريقة تدعو إلى تضليل الجمهور، ويمتد التجريم إلى كل من استعمل العلامة المقلدة أو المزورة بدون قصد، ووضعها بسوء نية على منتجاته.

يعطي القضاء في هذه الحالة، مالك العلامة التجارية الحق في رفع دعوى التقليد، لكي يستطيع نقل العنوان الإلكتروني أو إلغاءه والحصول على تعويض، لجبر ما حاق به من ضرر.

ويدين القضاء أيضا القرصنة إذا وقعت على اسم مقاطعة أو مدينة معينة تم تسجيلها من قبل.

ولا يحول دون الحكم بالإدانة عن جريمة القرصنة الإلكترونية أن يختلف المجال الذي تم تسجيل العنوان الإلكتروني فيه، عن المجال الخاص بالعلامة التجارية، فلمالك العلامة الحق في أن يسجلها في كل المجالات سواء أكانت دولية أو وطنية، وهناك العديد من القضايا أقر فيها القضاء بهذا المبدأ.[1]

لكي يجوز القول بوجود تقليد للعلامة الإلكترونية، ينبغي لقيام الجريمة أن يحدث ذلك تضليلا للجمهور، بحيث يلبس عليه الأمر بين العلامة الأصلية وتلك المقلدة، ويعود تقدير مدى مطابقة محتوى الموقع الإلكتروني للمنتجات التي تمثلها العلامة التجارية لقاضي الموضوع، حسب كل حالة على حدة.

يتفق الفقه والقضاء في فرنسا ومصر، في أن تقدير الخلط أو اللبس الذي يتركه تقليد العلامة التجارية في الأذهان، يجب أن يستند إلى النظرة العامة للعلامتين الأصلية والمقلدة، دون الحاجة للنظر إلى الجزئيات الصغيرة التي تتكون منها العلامتان، ويطبق هذا المبدأ عند نظر دعوى التقليد المتعلقة بالعناوين الإلكترونية.

[1] شريف محمد غنام، المرجع السابق، ص116.

فيما يخص العلامة التجارية المسجلة والسابقة على العنوان الإلكتروني، يعتبر القضاء مجرد تسجيل العنوان الإلكتروني قرصنة للعلامة التجارية، وله في ذلك حججه.[1]

أما بالنسبة للعلامة التجارية المسجلة بعد تسجيل العنوان الإلكتروني على شبكة الانترنت، فإن القضاء في هذه الحالة يحمي العنوان الإلكتروني، ويكيفه على أنه علامة تجارية، يجب حماية حق صاحبها على غرار الحماية التي يتمتع بها مالك العلامة التجارية.[2]

ثانيا: التنازع بين اسم النطاق وغيره من مواضيع القانون.

ليست العلامات التجارية وحدها هي محل التنازع مع اسم النطاق، حيث أنه من الممكن أن يحدث تنازع بين اسم النطاق والاسم التجاري أو الاسم الاجتماعي لمؤسسة أو حزب سياسي أو جمعية مدنية أو اسم المحل التجاري لشركة معينة قد تمتلك العديد من المحلات التجارية، كما أنه من الممكن أن يقع الاعتداء على حق المؤلف، وذلك في الفرض الذي يقدم فيه أحدهم بتسجيل اسم مصنف محمي (عنوان مجلة أو اسم برمجية) كاسم للنطاق، وفي هذه الحالة يجوز اللجوء إلى القضاء بدعوى التقليد، وهذا ما قضت به محكمة استئناف باريس في قرار لها بتاريخ 17 فيفري 2006 حول النطاق carview.com والذي اعتبرته مكونا جنحة تقليد لأنه استعمل اسم برنامج carview كاسم نطاق، وهذا رغم غياب خطر اللبس لأن قانون المؤلف لا يعترف بمبدأ التخصص خلافا للعلامة التجارية.[3]

---

[1] ذلك أن مالك العلامة لا يمكنه تسجيل عنوان على شبكة الانترنت يمثل علامته، ومن التطبيقات القضائية لهذا الأمر قضية lafayette، حيث أكدت محكمة باريس الابتدائية في حكم لها سنة 1999 أن مجرد تسجيل العنوان الإلكتروني galaries-lafayette.com، يعني أن الشركة المسجلة حجزت لنفسها موقعا بالاسم ذاته، ومنعت الشركة الأصلية من الاستفادة منه، مما يشكل تقليدا للعلامة الأصلية، والحكم ذاته نجده في قضية sfr، وكذا قضية l'oréal. كما اعتبر القضاء الفرنسي أن كتابة عبارة موقع تحت الإنشاء استغلال للموقع، من ذلك حكم محكمة ليل الابتدائية سنة 2000 الذي اعتبر هذا الأمر يشكل جنحة تقليد للعلامة التجارية الخاصة ب kiloutou. كما أن مركز التحكيم التابع لمنظمة التجارة العالمية Ompi، أكد أن مجرد عرض الموقع الالكتروني للبيع بعد تسجيله يعد استعمالا بسوء نية مما تقوم معه جريمة تقليد العلامة التجارية وفقا للفقرة الثالثة من المادة الرابعة من قواعد udrp.بشريف محمد غنام، المرجع السابق، ص134 وما بعدها.

[2] من أمثلة ذلك الحكم الصادر عن محكمة مينز الابتدائية سنة 1999 بخصوص نزاع بين شركة SFDI التي قامت باستخدام العلامة océant على شبكة الانترنت وفقا لنظام IP، السابق على العنوان الإلكتروني، وشركة Microvaz، التي ادعت بأن الشركة الأولى اعتدت على علامتها التجارية بتسجيلها كعنوان إلكتروني. في هذه القضية كان النزاع بين عنوان إلكتروني سجلته شركة، وبين علامة تجارية مملوكة لشركة أخرى تم تسجيلها بعد تسجيل العنوان الإلكتروني. وكان التساؤل المطروح: من يعلو على الآخر: العنوان الإلكتروني المسجل سابقا أم العلامة التجارية المسجلة لاحقا؟ اعتبرت المحكمة الفرنسية النزاع بين علامتين تسبق إحداهما الأخرى في التسجيل، وعليه يجب حماية العلامة الأسبق (العنوان الإلكتروني)، والحكم ذاته قضي به في قضايا مماثلة. انظر شريف محمد غنام، المرجع السابق، ص142وما بعدها.

[3] Romain v.gola. op cit. p97.

ثالثا: تسوية المنازعات بين مسجلي أسماء النطاق ومالكي العلامات التجارية

عموما، يتم تسوية المنازعات التي قد تثور بين مالكي العلامات التجارية ومسجلي أسماء النطاق، بطريقين: عن طريق الدعاوى القضائية، وعن طريق الوسائل غير القضائية، وما يهمنا أكثر هو الوسائل القضائية.

بخصوص الدعاوى القضائية نميز بين نوعين من الدعاوى: الدعاوى القضائية العامة، والدعاوى القضائية الخاصة، فالأولى أي العامة هي تلك الدعاوى المستندة على القواعد القانونية العامة، والتي لم توضع خصيصا لمعالجة الاعتداءات على العلامات التجارية على شبكة الانترنت،[1] أما الدعاوى الثانية أو الخاصة فهي تلك الدعاوى التي تستند إلى نصوص قانونية خاصة بحماية العلامات التجارية على شبكة الانترنت، وأول هذه النصوص القانونية هو قانون حماية المستهلك ضد القرصنة الإلكترونية الأمريكي الصادر في 29 نوفمبر 1999.[2]

1- الدعاوى القضائية العامة

لحماية العلامة التجارية من اسم النطاق يجوز رفع دعوى تقليد العلامة، ودعوى المنافسة غير المشروعة.

أ- دعوى تقليد العلامة التجارية

هي دعوى جزائية تهدف إلى توقيع الجزاءات الجنائية ضد كل معتد على العلامات التجارية بتزويرها أو تقليدها أو استعمالها بعد تزويرها، وتنص على ذلك م113 من قانون الملكية الفكرية المصري، وم32 من الأمر 06/03 الصادر في 19 يوليو 2003 المنظم للعلامات التجارية.[3] ومن شروط رفع هذه الدعوى أن تكون العلامة التجارية مسجلة لدى المعهد الوطني للملكية الصناعية (م5 من الأمر 06/03 سالف الذكر)، وضمن مدة الحماية المقررة بعشر سنين قابلة

[1] شريف محمد غنام، المرجع السابق، ص 157.

[2] المرجع نفسه، ص 180.

[3] ج ر المؤرخة في 23 يوليو 2003. عدد 44

للتجديد، كما يشترط أن يتم التقليد للعلامة المسجلة بالجزائر داخل إقليم الجزائر، أو أن تكون العلامة محمية بموجب اتفاقية أو معاهدة منظمة إليها الجزائر.[1]

الجدير بالتنويه بخصوص جريمة تقليد العلامات التجارية عبر شبكة الانترنت، أنها في المنازعات التي تثور بين مالكي العلامات التجارية ومسجلي أسماء النطاق (العناوين الإلكترونية)، فإن الهدف من الدعوى ليس توقيع الجزاء الجنائي على مرتكب التقليد، وإنما رد الاعتداء الواقع على العلامة التجارية عن طريق إلغاء تسجيل اسم النطاق ونقله إلى مالك العلامة الأصلية،[2] والحصول على تعويض نتيجة الاعتداء، مما يجعل دعوى التقليد أقرب للدعوى المدنية من الجنائية.[3]

ولكي تقوم جنحة التقليد لا بد لمالك العلامة أن يثبت ملكيته للعلامة التجارية المستوفية للشروط القانونية، بتقديم شهادة تفيد التسجيل الوطني أو الدولي للعلامة، كما يجب أن يوجد تقليد حرفي، وهو نقل حرفي للعلامة التجارية دون تغيير، بحيث يطابق اسم النطاق العلامة التجارية (واصطلح عليه المشرع المصري لفظ التزوير في م113 من قانون الملكية الفكرية)، أو تقليد شبه حرفي للعلامة التجارية من قبل مسجل اسم النطاق (وهو ما اصطلح عليه المشرع المصري لفظ تقليد في م113)، والعبرة في تقدير التقليد الحرفي أو شبه الحرفي بالمظهر العام لاسم النطاق، حتى لو اختلف مع العلامة التجارية في بعض العناصر المكونة لهما،[4] ويشترط أيضا لقيام جنحة التقليد أن يوجد

---

[1] بن دريس حليمة، جريمة تقليد العلامات التجارية، مذكرة تخرج لنيل شهادة الماجستير في القانون الخاص، جامعة أبي بكر بلقايد تلمسان، 2008، ص66.

[2] مثال ذلك الحكم الصادر من محكمة باريس في 2015/03/16 عن طريق أمر استعجالي.

La société de services qui apparaît comme le titulaire des noms de domaine qu'elle aurait dû enregistrer pour le compte de sa cliente a été condamnée à les lui transférer, par une ordonnance de référé rendue par TGI de Paris, le 16 mars 2015.

Le salon de thé et épicerie fine Tea Adoro est titulaire de quatre marques. Il a Le tribunal a estimé que l'impossibilité pour le salon de thé Tea Adoro de continuer à exploiter ses marques et plus précisément son activité de ventes en ligne, du fait qu'il n'avait plus la main sur ses noms de domaine, constitue un trouble manifestement illicite qui justifie l'injonction de transfert. Le prestataire est par ailleurs condamné à rembourser son client des sommes qu'il a dû avancer pour le développement d'un nouveau site par un autre prestataire et l'enregistrement de nouveaux noms de domaine.

confié à la société Millenium la conception du design de ses produits, de son identité visuelle et de deux sites internet. Tea Adoro lui avait également demandé de réserver pour son compte cinq noms de domaine reprenant ses marques. Or, le whois des différentes extensions fait apparaître Millenium comme titulaire. Tea Adoro a donc rompu ses relations commerciales avec son prestataire, d'autant plus que le site n'a pas été opérationnel. Voir le site : légalis.net.

[3] شريف محمد غنام، المرجع السابق، ص159. غير أن الجزاءات الموقعة بسبب جنحة التقليد، خاصة في الدول التي لا تملك تشريعا خاصا بالانترنت، هي جزاءات جنائية، أبرزها العقوبات السالبة للحرية والغرامة، مما يدعو إلى القول أن دعوى التقليد جزائية صرفة وليست مدنية.

[4] المرجع نفسه، ص160.

مخاطر للخلط أو اللبس في أذهان المستهلكين بين العلامة التجارية واسم النطاق، قد تترتب عليه أضرار لمالك العلامة، ويترك تقدير مدى هذا اللبس في أذهان الجمهور إلى تقدير القاضي اعتمادا على التماثل والتشابه الموجود بينهما، وفق ظروف كل حالة على حدة،[1]وفي القانون الفرنسي إذا كانت العلامة مشهورة أو مسجلة في الفئة 38 فإنها تستحق الحماية دونما حاجة إلى وجود الالتباس في ذهن الجمهور، وقد حكمت محكمة فرنسية بوجود تقليد بمجرد استعمال العلامة التجارية pacanet عبر الانترنت دون ترخيص من مالكها، لأنها مسجلة ضمن الفئة 38،[2] والأمر نفسه بالنسبة لقضية "فيشي"، حيث اعتبرت المحكمة أن هناك تعديا على العلامة فيشي المسجلة في الفئتين 3 و5، من قبل الشخص الذي سجل اسم النطاق vichy.com باعتبار أن العلامة المذكورة مشهورة.[3]

ب- دعوى المنافسة غير المشروعة.

يرى الفقه الراجح أن دعوى المنافسة غير المشروعة عبارة عن دعوى مسؤولية عادية، أساسها فعل المنافسة غير المشروع، الذي يعتبر خطأ يلزم من ارتكبه بتعويض من حاق به ضرر جراء ارتكاب هذا الفعل غير المشروع، طبقا للقواعد العامة المتعلقة بالمسؤولية عن العمل غير المشروع، بيد أن هناك جانبا آخر من الفقه يؤسس دعوى المنافسة غير المشروعة على أسس أخرى تتفق وطبيعتها حسب رأي هؤلاء الفقهاء الذين اختلفوا بينهم حول هذا الأساس المعتمد،[4] ومهما يكن فإن

---

[1] المرجع نفسه، ص 161.

[2] نصير الدين حسن أحمد، عناوين مواقع الانترنت، تسجيلها وحمايتها، تنازعها مع الماركات التجارية، دراسة مقارنة، منشورات زين الحقوقية، بيروت، لبنان، 2008، ص 239.

[3] المرجع نفسه، ص240.

[4] بن دريس حليمة، المرجع السابق، ص 123 وما بعدها.

يؤسس جانب من الفقه المنافسة غير المشروعة على أنها مساس بحق التاجر على العملاء وعلى ملكية المحل التجاري، لذلك فإن الطرق المستخدمة لتحويل العملاء تعتبر اعتداء على هذا الحق، غير أن جانبا آخر من الفقه يرى أن دعوى المنافسة غير المشروعة لا تقوم إلا في حالة تحويل العملاء بأساليب غير مشروعة. ويؤسس بعض الفقه دعوى المنافسة غير المشروعة على نظرية التعسف في استعمال الحق، غير أن فريقا آخر من الفقه لا يوافق على ذلك، باعتبار أن انظرية التعسف في استعمال الحق لا تعدو أن تكون خطأ موجبا للمسؤولية التقصيرية وفقا لأحكام م124 من القانون المدني، ولا يجوز تطبيق هذه النظرية على المنافسة غير المشروعة لأسباب منها أن التعسف في استعمال الحق لا يسعى إلى فائدة كبيرة على عكس المنافسة غير المشروعة، ناهيك عن أن المنافسة غير المشروعة لا تقوم بتحويل الحق عن وظيفته بغرض الإضرار بالمنافس كما هو الشأن بالنسبة للتعسف في استعمال الحق.

ولقد تطرق المشرع الجزائري إلى الممارسات التجارية غير النزيهة (ويقصد المنافسة غير المشروعة)، في نص المادة 26 من الأمر 04-02. لمزيد من التفصيل يراجع: بن دريس حليمة، حماية حقوق الملكية الفكرية في التشريع الجزائري، أطروحة دكتوراه في القانون الخاص، جامعة أبي بكر بلقايد، تلمسان، 2014/2013، ص138 وما بعدها.

الأحكام القضائية استقرت على جعل المسؤولية التقصيرية أساسا لهذه الدعوى، التي يشترط لقبولها أن تكون المنافسة غير مشروعة، وأن يلحق ضرر بالمدعي عليه نتيجة لذلك.[1]

من خلال التطبيقات القضائية تبين أن اللجوء إلى دعوى المنافسة غير المشروعة يتم بشكل أكبر في حالة وجود اعتداء على الاسم التجاري أو الأسماء الشخصية وأسماء الأسر، أما في حالة وجود اعتداء على العلامات التجارية فيلجأ إليها في حالة عدم وجود تقليد للعلامة التجارية، كما هو الحال في قضية شركة "مارك لوران" للألبسة الرجالية، والمالكة للاسم التجاري والعلامة التجارية celio والمسجلة في الفئة الخاصة بالملبوسات والتي ادعت على مسجل اسم النطاق celio.com، ورأت المحكمة أن لا وجود لجريمة التقليد باعتبار العلامة غير مسجلة في الفئة 38، ولكنها حكمت بوجود اغتصاب للاسم التجاري وتعسف باستعمال حق حجز اسم النطاق، وحرمان مالك العلامة من مكنة استغلاله للتعريف عن نفسه عبر الانترنت.[2] وهنا اعتبرت المحكمة أن الخطأ المكون للفعل غير المشروع، والذي يعتبر أساسا لقيام دعوى المنافسة غير المشروعة، هو التعسف في حرية تسجيل اسم النطاق، وليس التعسف في استخدام هذا الاسم كما تقرر القواعد العامة.[3]

كما أن القضاء الفرنسي أقام الخطأ في دعوى المنافسة غير المشروعة على فكرة التذويب أو dilution، وقد استلهمها من القانون الأمريكي، ويعني التذويب التقليل من الطبيعة المميزة للعلامات المشهورة،[4] عن طريق التقليل من قدرتها على تعريف وتمييز البضائع أو الخدمات،[1] وهو

---

[1] المرجع نفسه، ص124.

[2] نصير الدين حسن أحمد، المرجع السابق، ص 243.

[3] شريف محمد غنام، المرجع السابق، ص 167.

[4] والسؤال الذي يتبادر إلى الذهن هنا: ما المقصود بالعلامة المشهورة؟ لم تتعرض معظم التشريعات إلى تعريف العلامات المشهورة، سواء على مستوى القوانين الوطنية أو الاتفاقيات الدولية، وتركت تلك المهمة للفقه والقضاء، واستثناء عرفتها بعض التشريعات الوطنية منها التشريع الأردني في المادة 2 من القانون رقم 29 لسنة 2007 الخاص بالعلامات التجارية بأنها: "العلامة التجارية ذات الشهرة العالمية، التي تجاوز شهرتها البلد الأصلي الذي سجلت فيه، واكتسبت شهرة في القطاع المهني من الجمهور..." كما عرفتها المادة 4/ف1 من قانون العلامات التجارية الاتحادي لدولة الإمارات العربية رقم 8 لسنة 2002 بأنها: "العلامة التجارية ذات الشهرة العالمية التي تجاوز حدود البلد الأصلي للعلامة إلى البلاد الأخرى..." أما الفقه فقد عرفها بتعريفات متعددة منها أنها: "العلامة التي فرضت نفسها على الجمهور بازدياد الاستعمال والدعاية التي كانت محلا لها" وعلى مستوى القضاء فإن محكمة استئناف باريس عرفتها في حكمها الصادر في 17 يناير 1996 بأنها: "العلامة المعروفة لدى عدد من الجمهور وتتمتع بسلطة جذب له، مستقلة عن المنتجات أو الخدمات التي تمثلها، ولها أهمية كبيرة لدى المستهلكين". كما أن الويبو في دورة مشتركة لجمعيات الدول الأعضاء فيها أرست منعقدة بين 20-25 سبتمبر 1999 وضعت قواعد أو معايير يمكن الاسترشاد بها لتحديد العلامة التجارية المشهورة. لمزيد من التفصيل حول العلامة التجارية

ثلاثة أنواع: التغشية، تشويه السمعة والتحريف؛ فالتغشية تعني استعمال علامة مشهورة مرتبطة بمنتج محدد، للترويج لمنتجات أخرى دون الحصول على ترخيص، ومن أمثلة ذلك استخدام العلامة kodac المشهورة في مجال الكاميرات والأفلام، على منتجات مختلفة عن ذلك مما يشتت تأثيرها وجاذبيتها في أذهان المستهلكين الذين ألفوها مرتبطة بمجال الأفلام والكاميرات؛ وتشويه السمعة يعني استعمال العلامة المشهورة في مجال آخر يسيء إليها كاستعمال علامة مشهورة للعطر من قبل شركة مختصة بنقل المجارير؛ أما التحريف فيحصل عندما تعمد إحدى الكيانات في مجال المقارنة الإعلانية بين العلامات إلى تحريف العلامة المملوكة من قبل الطرف الآخر وتقديمها إلى المستهلكين بشكل محرف أي مخالف لحقيقتها، سواء أتم ذلك عن سوء أو حسن نية.[2]

اعتبر القضاء الفرنسي أن مجرد تسجيل علامة تجارية مشهورة في صورة اسم نطاق من قبل الغير يعتبر تذويبا،[3] ويصف القضاء الضرر الواقع على العلامة التجارية في هذه الحالة بأنه ضرر في صورة العلامة préjudice d'image يتمثل في ضياع ثقة الجمهور في العلامة التجارية؛ فحينما يرغب مستعمل الانترنت في الوصول إلى موقع الشركة، يفاجأ أن الموقع لا يخص الشركة التي قصدها وإنما شركة أخرى، أو يجد عبارات من مثل: الموقع غير متاح، أو موقع خطأ، أو يجد صفحة الموقع خالية من أية معلومات، أو بها إعلانات لشركة منافسة، مما يؤدي في النهاية إلى فقدان العلامة لأهميتها في أذهان المستهلكين، ومن التطبيقات القضائية لهذا الأمر، قضية "فيشي"، التي أكدت المحكمة بصددها أن تسجيل اسم النطاق vichy.com جعل متعاملي الانترنت الذين يزورون هذا الموقع بغية الإطلاع على منتجات "فيشي" التي تملكها الشركة "لوريال"، لا يجدون هذه المنتجات مما يجعل شركة "لوريال" تصاب بضرر ينبغي على من تسبب فيه جبره على أساس المسؤولية التقصيرية، والأمر نفسه نجده بالنسبة لقضية guy laroche حيث أسست المحكمة خطأ المدعي عليه المسجل لاسم النطاق guylaroche.com على فكرة الضرر، المتمثل في أن متعاملي شبكة الانترنت يجدون على صفحة الموقع عبارة خطأ، مما يفقد الشركة المدعية ثقة المستهلك في اسمها ومنتجاتها.[4]

المشهورة يراجع: نهى خالد عيسى، العلامة التجارية المشهورة، دراسة مقارنة، مجلة جامعة بابل للعلوم الانسانية، المجلد 21، العدد1،2013، ص42 وما بعدها.

[1] نصير الدين حسن أحمد، المرجع السابق، ص 253.

[2] نصير الدين حسن أحمد، المرجع السابق،ص ص258- 259.

[3] المرجع نفسه، ص259- 260، وانظر أيضا: شريف محمد غنام المرجع السابق، ص 164.

[4] شريف محمد غنام، المرجع السابق، ص 166.

انتقد جانب من الفقه منحى القضاء الفرنسي في اعتباره مجرد تسجيل علامة مشهورة يعتبر تذويبا، لأن في ذلك توسعا خطيرا، وتحيزا لأصحاب العلامات المشهورة، مما دفع المحاكم إلى اعتماد بعض المعايير الإضافية لإثبات أن هناك حالة لبس، ومنها أن توجد درجة كافية من الشبه بين علامة المستعمل الأول وعلامة أو اسم نطاق المستعمل الحديث، يجوز القول معها بوقوع ضرر اقتصادي فعلي لقيمة العلامة المشهورة، من خلال تقليل قدرتها البيعية المكونة سابقا كأداة دعائية للبضائع أو الخدمات المستعملة عليها،[1] وتطبيقا لذلك، فإن محكمة باريس الابتدائية في حكم لها بتاريخ 16 أكتوبر 2001، بشأن قضية Air France حكمت بأن الضرر الذي سببه تسجيل اسم النطاق air France.com من جانب السيد "F "والشركة الإنجليزية "interdartlimited " كان محدودا، إذ أن الموقع لم يستغل منذ 1996، ولا يتضمن أية معلومات تضر بصورة العلامة air france، في نظر عملائها.[2] وهنا اعتمدت المحكمة على معيار الضرر الواقع على صورة العلامة في نظر عملائها.

والجدير ذكره أن دعوى المنافسة غير المشروعة قد يكون لها دور تكميلي، بمعنى أنه يجوز رفعها إلى جانب رفع دعوى التقليد، وتستند في هذه الحالة إلى الوقائع التي استندت لها دعوى التقليد،[3] وقد يكون لدعوى المنافسة غير المشروعة دور أصيل، أي مستقل عن دعوى التقليد في الحالات التي لا تنطبق فيها دعوى التقليد لعدم توافر شروطها، من مثل حالة العلامة التجارية غير المسجلة والتي هي محل استعمال من قبل صاحبها، أو العلامة التجارية التي لم يتم تجديد تسجيلها، أو بسبب تقادم دعوى التقليد.[4]

أما الجزاءات القضائية الموقعة استنادا إلى هذه الدعاوى القضائية العامة فأهمها:[5]

[1] نصير الدين حسن أحمد، المرجع السابق، ص 261.

[2] شريف محمد غنام، المرجع السابق، ص 166.

[3] المرجع نفسه، ص163.

[4] المرجع نفسه، ص162.

[5] المرجع نفسه، ص 170 وما بعدها.

– وقف استخدام اسم النطاق أي حظر استعماله في أي نشاط كان لحين الفصل في مصيره، كما يحظر على مسجل اسم النطاق استغلال اسم نطاق آخر بالاسم نفسه أو باسم مشابه له تحت طائلة الغرامة التهديدية.

– إلغاء أو نقل اسم النطاق، وهنا تثور مسألة تحديد الجهة التي يخاطبها الحكم، وهي الجهات المكلفة بتسجيل أسماء النطاق على الانترنت، ومنها ما هو وطني يتبع الدولة التي صدر فيها الحكم، ومنها ما هو دولي، ومبدئيا نعلم أن الحكم الصادر في النزاع بين مالك العلامة ومسجل اسم النطاق لا يلزم إلا طرفيه، غير أن الجهات المكلفة بتسجيل أسماء النطاق غالبا ما تستجيب طواعية لأحكام القضاء الذي تنبه لهذا الأمر، فأصبح يوجه مجرد مخاطبات للشركة المكلفة بالتسجيل، بإلغاء أو نقل اسم النطاق، تاركا لها حرية التقدير.

– التعويض لجبر الضرر الذي تعرض له مالك العلامة من قبل مسجل اسم النطاق، حسب نوع ومقدار الضرر، وتقدير ذلك للقضاء.

– نشر الحكم الصادر بالإدانة كعقوبة تكميلية، ومن المستحسن في مثل هذه القضايا أن يكون النشر على شبكة الانترنت من خلال الموقع الخاص بالشركة المدعى عليها، أو الشركة المدعية، ومن ذلك الحكم الصادر في قضية saint tropez حيث أمرت المحكمة بنشر الحكم كله على الصفحة الأولى لموقع شركة eurovirtuel.

بالإضافة إلى الجزاءات الواردة في قوانين الملكية الفكرية والخاصة بجنحة التقليد وأهمها العقوبات السالبة للحرية والغرامات المالية.

2- الدعاوى القضائية الخاصة

يقصد بها تلك الدعاوى المستندة إلى قانون خاص، وخير مثال لها القانون الأمريكي لحماية المستهلك من القرصنة الإلكترونية، الصادر في 29 نوفمبر 1999 والذي بدأ نفاذه منذ يناير 2000، وأهم ما جاء فيه، إدانة القرصنة الإلكترونية اعتمادا على سوء نية مسجل اسم النطاق، دون أخذ في الاعتبار تماثل أو تشابه المنتجات والخدمات التي تمثلها العلامة التجارية واسم النطاق، وحدد القانون تسع حالات لسوء نية المسجل، يكفي توافر إحداها. كما أعطى القانون مالكي العلامات التجارية مكنة رفع دعوى خاصة، وفق شروط معينة، ضد مسجلي أسماء النطاق، تسمى الدعوى

العينية، تقتصر مهمة المحكمة فيها على الأمر بإلغاء تسجيل اسم النطاق، أو نقله إلى مالك العلامة التجارية.[1]

3- التسوية غير القضائية لمنازعات أسماء النطاق

يطلق عليها أيضا التسوية الودية، والهدف منها تجنب الإجراءات القضائية الطويلة، وكذا تجنب الإزعاج والتشويش الذي قد يحدث في أذهان الجمهور بسبب النزاع بين مالك العلامة التجارية، ومسجل اسم النطاق، وحل المشكل بطريق سريع، يتلاءم وطبيعة العالم الرقمي.

بإمكان مالك العلامة التجارية اللجوء إلى المفاوضات مع مسجل اسم النطاق، وعادة ما تكون عبر موقعه الإلكتروني، طالبا منه التنازل عن اسم النطاق لصالحه، في حالة استجابة المسجل لاسم النطاق لمطلب صاحب العلامة التجارية المتضرر، فإنه غالبا ما يطلب منه مبلغاً من المال ليتنازل عن اسم النطاق له، قد يكون هذا المبلغ مناسبا فيوفر صاحب العلامة التجارية على نفسه عناء رفع شكاوى أمام إحدى الجهات التي تحل منازعات أسماء النطاق. أما إذا كان المبلغ كبيرا وهذا الذي يحدث في الغالب خاصة إذا كانت الشركة التي تملك العلامة التجارية مرموقة، فإن الإجراء الأمثل يكمن في الالتجاء لإحدى الجهات التي تحل منازعات أسماء النطاق.[2]

كما يمكن لمالك العلامة التجارية مراقبة وقت انتهاء اتفاقية تسجيل اسم النطاق، المبرمة بين الشخص المسجل لعلامته التجارية والجهة التي تقدم خدمات تسجيل أسماء النطاق، ويستغل عدم تجديد المسجل اتفاقية التسجيل، فيسجل اسم النطاق الذي انتهت فترة تسجيله باسمه، ولكن هذا الإجراء غير مضمون ونادرًا ما يغفل مسجل اسم النطاق عن تجديد تسجيله للاسم، خصوصاً إذا ما كانت العلامة التجارية التي يحتويها اسم النطاق تعود لشركة ذات سمعة طيبة.[3]

في حالة وجود منازعة حول العلامة التجارية واسم نطاق وطني، يجوز أن يلجأ صاحب العلامة التجارية المتضرر لحل منازعته وفقا للسياسات التي تضعها الجهات المسؤولة عن التسجيل،

---

[1] شريف محمد غنام، المرجع السابق، ص184 وما بعدها.

[2] رامي محمد علوان، المنازعات حول العلامات التجارية وأسماء مواقع الانترنت، مجلة الشريعة والقانون، العدد22، يناير 2005، ص300.

[3] المرجع نفسه، ص301.

والتي قد لا تتبع السياسة الموحدة لحل منازعات أسماء مواقع الانترنت، وقد طورت بعض الجهات المسؤولة عن تسجيل أسماء النطاق الوطنية إجراءات خاصة لحل المنازعات.[1]

كما يجوز لمالك العلامة التجارية اللجوء إلى القواعد العامة لتسوية منازعات أسماء النطاق "UDRP" [2] التي أصدرتها "الأيكان" في 24 أكتوبر 1999 ودخلت حيز التنفيذ في فاتح يناير 2000. وقد تضمنت هذه القواعد إجراءات إدارية ودية لتسوية المنازعات بشكل ودي وأقل تكلفة،[3] ولكن ينبغي توافر شروط معينة حتى يجوز اللجوء إلى مثل هذه القواعد، منها أن يتطابق اسم النطاق مع العلامة التجارية أو يتشابه معها بصورة مشوشة لأذهان عملائها، وألا يكون لمسجل اسم النطاق حق أو مصلحة مشروعة على هذا الاسم، وفق ما حددته المادة 4 الفقرتان:b وc من القواعد العامة لتسوية المنازعات.[4]

[1] المرجع نفسه، ص303.

[2] Uniforme Dispute Resolution Policy.

[3] شريف محمد غنام، المرجع السابق، ص 193.

[4] خليفي مريم، العناوين الإلكترونية والعلامات التجارية في مجال التجارة الإلكترونية: روابط ونزاعات، مجلة دراسات وأبحاث، العدد2، جامعة الجلفة، الجزائر2010،ص ص159-160.

الفصل الثاني: الحماية الجزائية للمستهلك في مجال التجارة الإلكترونية.

المستهلك[1] في مجال التجارة الإلكترونية، يطلق عليه الفقه عادة المستهلك الإلكتروني أو الرقمي،[2] حيث أنه لا يعدو أن يكون مستهلكا عاديا، ولكن الوسيلة التي يتعامل عبرها مع الشركات والأشخاص إلكترونية، وهذا فرق له خصوصياته وتترتب عليه نتائج هامة؛[3] فالمستهلك الإلكتروني يتمتع بالحقوق نفسها التي يتمتع بها المستهلك في عقود التجارة التقليدية إضافة إلى حقوق أخرى أملتها طبيعة التعاقد الإلكتروني، تتعلق بمسائل هامة من مثل ضرورة إحاطته علما بالبيانات والمعلومات اللازمة المتعلقة بالبائع والسلعة، والثمن وطرق الدفع، وشروط الضمانات التجارية، وكافة مراحل إنجاز المعاملة التجارية، ومدى حماية المستهلك الإلكتروني من الإعلانات الكاذبة والخادعة، وكذا مسألة سرية البيانات الخاصة بالمستهلك الإلكتروني، إذ قد يتعرض هذا المستهلك إلى انتهاك بعض من خصوصياته الشخصية أثناء المعاملة الإلكترونية، والمدة المحددة للاحتفاظ بتلك البيانات، ومدى حق المستهلك في فسخ العقد، وأمور أخرى مدنية وجزائية تفرض نفسها وتدعو إلى فرض حماية متميزة للمستهلك الإلكتروني.[4]

يعالج هذا الفصل موضوع الحماية الجزائية للمستهلك الإلكتروني من جرائم الأموال (المبحث الأول)، ثم الحماية الجزائية للحق في الخصوصية للمستهلك الإلكتروني(المبحث الثاني).

---

[1] تضفي معظم التشريعات المقارنة بطريقة مباشرة أو ضمنية، صفة المستهلك على الأشخاص الطبيعيين الذين يتصرفون لغايات غير مهنية، وتختلف فيما بينها على إسباغ هذه الصفة على الأشخاص المعنوية وعلى الأشخاص الطبيعيين الذين يتصرفون لغايات مهنية في غير تخصصهم. ومن خلال استقراء نصوص القانون الفرنسي نجده يتوسع في إضفاء هذه الصفة على كل هؤلاء خاصة إذا تعلق الأمر بالبيع عن بعد (التجارة الإلكترونية) والقروض الاستهلاكية، والشروط التعسفية. يراجع: د. يوسف شندي، المفهوم القانوني للمستهلك، دراسة تحليلية مقارنة، مجلة الشريعة والقانون، العدد44، أكتوبر 2010، ص 142 وما بعدها.

[2] وضعت القوانين المقارنة جملة من المبادئ لحماية المستهلك في مجال التعاملات الإلكترونية، من بينها ذكر البيانات الهامة عند الإعلان عبر الوسائل الإلكترونية، احترام سرية البيانات الخاصة بالعملاء واعتبار العقود النمطية المبرمة عن بعد من عقود الإذعان. لأكثر تفصيل يراجع: هدى حامد قشقوش، المرجع السابق، ص 66 وما بعدها.

[3] منها تحديد القانون الواجب التطبيق على الواقعة، فالمستهلك الإلكتروني يحكمه علاوة على القواعد العامة في حماية المستهلك العادي، قواعد قانونية خاصة بحماية التعاملات الإلكترونية، وكذلك القواعد الدولية المنظمة للمعاملات والتجارة الإلكترونية، كما أن المستهلك الإلكتروني يتعاقد على سلعة لم يرها، وهذا كفيل أن يجعله عرضة للغش والاحتيال...يراجع: د علي أحمد صالح المهداوي، أثر خيار الرؤية في حماية المستهلك الإلكتروني، مجلة الشريعة والقانون، العدد 42، أبريل 2010، ص193 وما بعدها.

[4] محمد خليفة، الحماية الجنائية للمستهلك في عقود التجارة الإلكترونية، المجلة التونسية، مركز النشر الجامعي، تونس 2009،ص ص187-188.

المبحث الأول: الحماية الجزائية للمستهلك الإلكتروني من جرائم الأموال.

يتناول هذا المبحث حماية المستهلك الإلكتروني ضد جرائم الأموال التقليدية (المطلب الأول)، ثم حمايته من الجرائم المستحدثة (المطلب الثاني).

المطلب الأول: الحماية الجزائية للمستهلك الإلكتروني من جرائم الأموال التقليدية.

يقصد بالجرائم التقليدية أو الكلاسيكية تلك الجرائم المعروفة، والتي ارتكبها الإنسان منذ القدم، أو تلك الجرائم التي صارت مألوفة لدى الناس نظرا لتكرار ارتكابها، ولعل من أبرزها جرائم السرقة والنصب وخيانة الأمانة... وقد تصدت التشريعات المقارنة لها بنصوص قانونية واردة في قانون العقوبات، والقوانين الملحقة به.

إن التطور المذهل للمعلوماتية وتطبيقاتها المتعددة في مجالات شتى، ومنها مجال التجارة الإلكترونية، أدى إلى ظهور مشاكل قانونية جديدة، شكلت أزمة حقيقية للقانون الجزائي إذ بات من الضروري عليه مواجهة واقع جديد هو واقع العالم الرقمي (الإلكتروني، الافتراضي) بكل مميزاته وخصائصه، بدون المساس بمبادئه المعروفة وعلى رأسها مبدأ شرعية الجرائم والعقوبات وما يتفرع عليه من ضرورة التفسير الضيق لقواعد القانون الجزائي، وحظر القياس في مجال التجريم والعقاب.

وعليه يطرح الإشكال التالي: إلى أي مدى تستطيع هذه القواعد العامة حماية المستهلك في مجال التجارة الإلكترونية دون المساس بمبادئها، خاصة مبدأ المشروعية؟[1]

الفرع الأول: السرقة والتجارة الإلكترونية.

يتم التطرق أولا إلى محل السرقة في التجارة الإلكترونية، ثم إلى صور وأركان السرقة في هذه التجارة.

[1] أمال قارة، المرجع السابق، ص 13.

أولا: محل السرقة في التجارة الإلكترونية.

تعرف السرقة حسب القواعد العامة على أنها "اختلاس مال منقول مملوك للغير، بنية تملكه".[1] وفي مجال التجارة الإلكترونية لا مشكلة إذا كان محل السرقة شيئا ماديا من مثل المكونات المادية للحاسب الآلي، أو آلات الطباعة، والأقراص الممغنطة وغيرها، ففي مثل هذه الحالة تطبق القواعد العامة الخاصة بالسرقة م350 ق ع، وم 350 مكرر1،[2] لأن محل السرقة شيء مادي منقول، غير أن الأمر يصبح دقيقا إذا كان محل السرقة إحدى المكونات المعنوية للحاسب الآلي، ومن أهمها المعلومات، ومن هنا يثور السؤال التالي: إلى أي مدى يجوز اعتبار المعلومات مالا منقولا؟ وبالتالي هل يجوز حمايتها وفق نصوص السرقة؟

أسالت محاولات الإجابة عن هذا السؤال الكثير من الحبر، بين رافضي اعتبار المعلومات محلا للسرقة ومؤيدي ذلك؛ فالاتجاه الرافض يدعم رأيه بالقول بأن المعلومات لا تصلح محلا للسرقة لطبيعتها، ولصعوبة إثبات كثير من الأفعال التي تقع عليها، ولا يجوز القياس على سرقة الكهرباء لأن ذلك يتعارض مع مبدأ الشرعية؛ [3] فالمعلومات ليست من قبيل الأشياء التي تحميها نصوص السرقة، كما أن المعلومات لا ترد عليها الحيازة كونها غير مادية، بالإضافة إلى أن هذه المعلومات تبقى مدونة على الدعامة التي تحملها رغم نسخها أو الإطلاع عليها، وفي ذلك تختلف عن المنقولات التي لا تبقى بعد تحريكها.[4] وهناك فريق من هذا الاتجاه يفرق بين المعلومات والبيانات التي تمت معالجتها إلكترونيا، حيث يجيز إعمال نصوص السرقة على هذه الأخيرة دون المعلومات، كون البيانات المعالجة إلكترونيا محددة في كيان مادي متمثل في نبضات أو إشارات إلكترونية ممغنطة بالإمكان تخزينها أو نقلها، وإعادة إنتاجها، وقياسها، وتقديرها من حيث الكم؛ فهي ليست أشياء معنوية كالآراء والأفكار، بل أشياء محسوسة وموجودة ماديا.[5]

---

[1] عبد الفتاح بيومي حجازي، التجارة الإلكترونية وحمايتها القانونية، المرجع السابق، ص175.

[2] أضيفت بالقانون 09-01 المؤرخ في 25 فبراير 2009، ج ر15، ص8. تطرقت هذه المادة إلى سرقة الممتلك الثقافي، مما يجعلنا نتساءل: هل يميل المشرع الجزائري إلى اعتبار المعلومات محلا للسرقة؟ يراجع: زيبحة زيدان، الجريمة المعلوماتية في التشريع الجزائري والدولي، دار الهدى، عين مليلة الجزائر2011، ص85.

[3] د. أحمد محمود مصطفى، المرجع السابق، ص282.

[4] بيومي حجازي، المرجع السابق، ص175.

[5] أمال قارة، المرجع السابق، ص18.

أما الاتجاه المؤيد لاعتبار المعلومات مالا وبالتالي يجوز أن تكون محلا لجريمة السرقة، لا يرى في الأمر أنه يتعارض مع المبادئ الأساسية للقانون الجنائي ومنها مبدأ الشرعية، إذ ليس من الضروري أن يكون المحل في جريمة السرقة ماديا، فالمشرع استعمل مصطلح شيء، الذي قد يكون ماديا أو معنويا، كما أن المعلومات أصبحت لها قيمة مالية واقتصادية كبيرة، تفوق بكثير الدعائم المادية التي تحملها، فكيف يسوغ إذن من حيث المنطق، تجريم سرقة هذه الدعائم المادية تافهة القيمة، وعدم تجريم سرقة المعلومات القيَمة التي عليها؟ كما أن سارق المعلومات يستأثر بواحدة من سلطات المالك على المعلومات، وهي حقه في إعادة إنتاجها دون أن يترتب عن ذلك نقل الشيء من مكانه، وفي حالة إذا كان للشيء قيمة معنوية فإن إعادة إنتاج المعلومات التي يحتوي عليها تفقد قيمة المعلومة التي تؤهلها لأن تكون محلا للسرقة وهي السرية،[1] خاصة وأن الواقع الجديد للعلاقات الاقتصادية يعتمد بشكل أساسي على المعلومات.

اتجه بعض الفقه الفرنسي إلى اعتبار المعلومات مجموعة مستحدثة من القيم، فهي منتج قائم على سعر السوق بصرف النظر عن دعامتها المادية، وترتبط بصاحبها عن طريق علاقة قانونية تتمثل في علاقة المالك بالشيء الذي يملكه.[2]

واتجه رأي فقهي آخر إلى اعتبار المعلومات مالا قانونيا، سواء أكانت مبتكرة أم لا، وهي جديرة بالحماية القانونية.[3]

ويميل فريق آخر من الفقه إلى القول بأن المعلومات لا يتحقق فيها وصف المال بالمعنى المتداول، وأن تسميتها الأموال المعلوماتية يتعين فهمها على أنها القابلية للاستغلال المالي لها.[4]

أما قضاء، فهناك أحكام عديدة، قضت بصلاحية المعلومات لأن تكون محلا للسرقة، من ذلك، إدانة محكمة النقض الفرنسية لعامل قام بنسخ أقراص ممغنطة بها معلومات هامة عن

---

[1] د. أحمد محمود مصطفى، المرجع السابق، ص284.

[2] د.أحمد خليفة الملط، المرجع السابق، ص239.

[3] المرجع نفسه، ص240.

[4] د. عمر فاروق الحسيني، لمحة عن جرائم السرقة من حيث اتصالها بنظم المعالجة الآلية للمعلومات، بحث مقدم لكلية الشريعة والقانون، في إطار بحوث مؤتمر القانون والكمبيوتر والانترنت، المنعقد من 1-3 سنة 2000، ط3، المجلد الأول، ص333.

العملاء، في قضية عرفت باسم: Bourquin،[1] وما قضت به محكمة استئناف ontario الكندية، وما حكمت به محكمة النقض المصرية التي اعتبرت المعلومات ذات القيمة الاقتصادية المتعلقة بالأسرار التجارية أو الصناعية، أو الأمن القومي جديرة بحماية القانون الجنائي.[2]

كما أن القضاء الفرنسي طبق قواعد جريمة الإخفاء في القضية الشهيرة ب:"يشيني" لمعاقبة المستفيد من المعلومات المميزة، وهذا كله يدعو إلى القول إلى صلاحية المعلومات لأن تكون محلا لجريمة السرقة.[3]

انطلاقا مما سبق يرفض جانب من الفقه إعمال النصوص التقليدية للسرقة لحماية المعلومات، وخاصة وأن المشرع حينما سن هذه النصوص، لم يكن في نيته ذلك، إلا أن الرأي الراجح هو جواز إعمالها لاسيما في ظل غياب منظومة نصوص خاصة كفيلة بضمان حماية أفضل للمعلومات. وفيما يخص النصوص الخاصة الموجودة والمتعلقة بنظم المعلومات عامة والتجارة الإلكترونية خاصة، فإنه في حالة التعدد المعنوي للجرائم يطبق القاضي العقوبة الأشد كما هو منصوص عليه في القواعد العامة للقانون الجنائي، كما لو تعددت جريمة السرقة مع جريمة الإخلال بحق المؤلف،[4] وكما في الفرض الذي يقوم فيه الجاني بسرقة برنامج معلوماتي أو التلاعب فيه، ثم استخدامه في سرقة الأموال عبر شبكة الإنترنت، فهنا يعاقب الجاني وفق العقوبة الأشد.[5]

ثانيا: صور وأركان السرقة في مجال التجارة الإلكترونية.

تتحقق السرقة في مجال التجارة الإلكترونية بصور تقنية مختلفة، ومن بينها: الالتقاط الذهني للمعلومات: بمعنى أن يتمكن الإنسان عبر حواسه الطبيعية من سماع أو قراءة للمعلومات من تخزينها في ذاكرته بهدف الاستفادة منها، ومن ذلك قراءة محرر أو مستند إلكتروني وحفظ فحواه،

---

[1] تتلخص وقائع الحكم في قيام مبرمج، كان قد ترك عمله في إحدى الشركات، إلى شركة أخرى، ثم قام بعد ذلك بزيارة إلى الشركة الأولى التي كان يعمل بها، وقام بتصوير أشرطة تتعلق بالعملاء الأثرياء الذين يتعاملون مع الشركة، على مطبعة الشركة، كما قام بأخذ شرائط أخرى نسخها بمعرفته على مطبعته، بهدف إنشاء شركة منافسة. حكمت عليه المحكمة بالحبس شهرا مع إيقاف التنفيذ بتهمة السرقة. أحمد خليفة الملط، المرجع السابق، ص253.

[2] د. أحمد محمود مصطفى، المرجع السابق،ص ص286-287.

[3] د. نائلة عادل محمد فريد قورة، المرجع السابق، ص183.

[4] د. شيماء عبد الغني، المرجع السابق، ص51.

[5] بيومي حجازي، المرجع السابق، ص199.

وبغض النظر عن مسألة صعوبة الإثبات، فإن جانبا من الفقه لا يرى مانعا من القول بسرقة المعلومات بهذه الطريقة،[1] النسخ غير المشروع للبيانات المخزنة إلكترونيا، ويجوز أن تطبق على هذه الجريمة أيضا قواعد نصوص حقوق الملكية الفكرية والأدبية، والالتقاط الهوائي للبيانات المعالجة أو المنقولة إلكترونيا أي التقاط الإشعاعات الكهرومغناطيسية الصادرة من أجهزة أخرى، أو التقاط الموجات القصيرة من نهاية طرفية إلى نهاية طرفية أخرى وترجمتها إلى بيانات مرئية عبر شاشة تلفزيونية.[2] كما قد يلجأ الجاني إلى إجراء توصيلات للجهاز للحصول على المعلومة، وعندها يقوم بتسجيل هذه المعلومات لديه، أو الإطلاع عليها دون تسجيلها، وقد يقوم بمحو المعلومة بعد الحصول عليها.[3]

يرى الفقه المؤيد لتطبيق قواعد السرقة على المعلومات أن فعل الاختلاس يرد على المعلومات محل السرقة، مثلما ترد السرقة على المنقول المادي في القواعد العامة، فالبرامج والمعلومات إنتاج فكري، وعليه فإن الحيازة في هذا النوع من الأموال هي حيازة فكرية وليست مادية، كما أن عدم رضا المجني عليه بإعطاء المعلومة يشكل الجانب الشخصي لفعل الاختلاس بالنسبة للسرقة في مجال التجارة الإلكترونية،[4] أما بالنسبة للركن المعنوي للجريمة فإن القصد الجنائي لا يتوافر لدى الجاني في السرقة إلا إذا توافرت لديه نية السرقة، مما يعني تطلب قصد جنائي خاص هو تملك الشيء محل الاختلاس، بالإضافة إلى القصد العام بعنصريه العلم والإرادة، العلم بأن الشيء محل السرقة مملوك للغير، وانصراف الإرادة رغم ذلك إلى اختلاس هذا الشيء. وفي مجال السرقة المعلوماتية ونظرا للطبيعة الخاصة للمعلومات يرى جانب من الفقه أن توافر نية الرد لا يحول دون توافر القصد الجنائي في سرقة المعلومات، حيث يكفي توافر نية التملك بصفة مؤقتة عليها استنادا إلى أن توافر نية الرد لا يحول دون توافر نية التملك إذا كان المال من طبيعته أن يهلك أو يفقد من قيمته، وأن الاستيلاء عليه يحرم صاحبه من الاستئثار به، وهذا هو الوضع بالنسبة للمعلومات.[5]

---

[1] أمال قارة، المرجع السابق، ص24.

[2] المرجع نفسه، ص26.

[3] د. محمود أحمد طه، المواجهة التشريعية لجرائم الكمبيوتر والانترنت، دراسة مقارنة، دار الفكر والقانون، المنصورة، مصر 2013، ص124.

[4] عبد الحليم بوقرين، الحماية الجنائية للمعاملات الإلكترونية، رسالة دكتوراه في القانون الخاص، جامعة أبي بكر بلقايد، تلمسان، 2014/2013، ص169.

[5] شيماء عبد الغني، المرجع السابق، ص54.

غير أن الفقه التقليدي يرفض هذه الحجج ويرى بأنه يصعب التوفيق بين الاستيلاء على المعلومات ونصوص جريمة السرقة؛ فالقول بالسرقة المؤقتة أو الظهور بمظهر المالك لا يتفق وطبيعة جريمة السرقة، خاصة وأن جرائم الأموال لا ترد على الخدمات والمنافع، لذلك ما من سبيل سوى تدخل المشرع لتجريم سرقة وقت الحاسب الآلي أو المنفعة للمعلومة الإلكترونية، كما فعل المشرع الإنجليزي.[1]

الفرع الثاني: جريمة النصب والاحتيال.

يتم التطرق أولا إلى مفهوم جريمة النصب بصفة عامة، ثم محاولة الإجابة عن السؤال التالي: إلى أي مدى يجوز أن تمتد الحماية المقررة للأموال وفق نص جريمة النصب إلى معاملات التجارة الإلكترونية؟

أولا: مفهوم جريمة النصب.

تقوم جريمة النصب والاحتيال[2] على الغش[3]الموصوف أو الغش المشدد، وهو الغش المحاط بحبك مسرحي للاستيلاء على أموال الغير. وحددت قوانين العقوبات أساليب هذا الغش على سبيل الحصر.[4] ويعرف النصب بأنه "كل كذب مصحوب بوقائع خارجية، أو أفعال مادية يكون من

---

[1] د. محمود أحمد طه، المرجع السابق، ص143.

[2] النصب والاحتيال مصطلحان لمعنى واحد من الناحية القانونية، فقد استعملت بعض الدول العربية في قوانينها مصطلح النصب كما هو الحال بالنسبة للجزائر ومصر والمغرب والبحرين، وأطلقت أخرى مصطلح الاحتيال مثل لبنان وسوريا والعراق والأردن، وفي فرنسا يستعمل المصطلح: "*l'escroquerie*". ولم تهتم التشريعات بتعريف جريمة النصب، وتركت ذلك للفقه، إلا أن بعضها قام بهذه المهمة ومنها قانون عقوبات البحرين في المادة 242 وقانون الجزاء الكويتي في المادة 231. وفي إيطاليا فقد عرف قانون العقوبات الإيطالي لسنة 1930 جريمة الاحتيال في المادة 460 . وقد أعطى الفقه عدة تعريفات للنصب أو الاحتيال منها: " جريمة الاحتيال هي كل فعل يباشره الجاني بنفسه أو بواسطة الغير، ويتوصل من خلاله إلى تسليم مال منقول مملوك للغير، بدون وجه حق، باستعمال وسائل الخداع التي نص عليها القانون، والتي يقع المجني عليه نتيجتها في الغلط الدافع للتسليم". انظر. الفريق. طاهر جليل الحبوش. جرائم الاحتيال. الأساليب والوقاية والمكافحة. أكاديمية نايف العربية للعلوم الأمنية. الرياض 2001. ص14 وما بعدها.

[3] يعرف الغش "*la fraude*" بأنه خداع يصدر من شخص ضد آخر بعد إبرام العقد أو وجود الالتزام، بقصد الإضرار بحقوق الغير. والغش بهذا المعنى يختلف عن التدليس، إذ أن هذا الأخير خداع يصدر من أحد المتعاقدين أثناء تكوين العقد، بقصد حمل الآخر على التعاقد معه. انظر: د. أبو الوفا محمد أبو الوفا. جريمة الغش في تداول الأسهم في القانون المقارن والفقه الإسلامي. بحث مقدم إلى مؤتمر أسواق الأوراق المالية والبورصات. كلية الشريعة والقانون. الإمارات العربية المتحدة.2006. ص1.

[4] د. أبو الوفا. المرجع السابق. ص28.

شأنها توليد الاعتقاد لدى المجني عليه بصدق هذا الكذب، مما يدفعه إلى تسليم ما يراد منه تسليمه، طواعية واختيارا".[1]

وقد تطرق المشرع الجزائري إلى جريمة النصب في المادة 372 ق.ع،[2] ومن أخطر جرائم النصب الإسهامُ في شركات تجارية وهمية، والاقتراضُ من البنوك بضمانات صورية، والتلاعبُ للحصول على تأمينات غير مستحقة، والاستيلاءُ على أموال المواطنين من خلال إيهامهم بمشاريع كبرى ذات أرباح طائلة[3]...وقد تتم هذه الصور عبر الوسائل الإلكترونية.

وتقوم جريمة النصب عموما على ركنين هما:

1- الركن المادي: وقوامه فعل الاحتيال بإحدى الطرق التي حددها القانون على سبيل الحصر، والنتيجة المترتبة عن هذا الفعل، والمتمثلة في تسليم الضحية مالا إلى الجاني، والعلاقة السببية بين الفعل المادي المتمثل في الاحتيال والنتيجة وهي الاستيلاء على مال الغير بغير وجه حق، 2 - الركن المعنوي والذي يستلزم توافر القصد الجنائي لدى الجاني والمتبلور في اتجاه إرادته إلى خداع المجني عليه والاستيلاء على ماله.[4]

وتقوم الجريمة حتى ولو لم يستول الجاني على الأموال لنفسه بل لغيره، تطبيقا لما هو مقرر في جريمة النصب، إذ لا تتطلب هذه الجريمة أن يحقق الجاني منفعة؛ وهذا ما قررته محكمة النقض الفرنسية حينما نصت بأن: "المادة 405 من قانون العقوبات لا تتطلب لإعمالها شرط أن تكون القيم محل عملية النصب قد آلت إلى حساب مرتكب الجنحة".[5]

---

[1] الفريق طاهر جليل الحبوش، جرائم الاحتيال، الأساليب والوقاية والمكافحة، أكاديمية نايف العربية للعلوم الأمنية، الرياض2001، ص26.

[2] يرى الدكتور أحسن بوسقيعة أن صياغة المادة 372 باللغة العربية لم يكن موفقا وجاء مبتورا ولا يؤدي المعنى الوارد في النسخة الفرنسية، ولذلك اقترح الصياغة التالية: "كل من توصل إلى استلام أو تلقي أموال أو منقولات أو سندات أو تصرفات أو أوراق مالية أو وعود أو مخالصات أو إبراء من التزامات أو إلى الحصول على أي منها أو شرع في ذلك، وكان ذلك بالاحتيال، لسلب كل ثروة الغير أو بعضها أو الشروع فيه، إما باستعمال أسماء أو صفات كاذبة، وإما باستعمال مناورات احتيالية لإيهام الغير بوجود سلطة خيالية أو اعتماد مالي خيالي، أو لإحداث الأمل في الفوز بأي شيء أو الخشية من وقوع حادث أو أية واقعة أخرى وهمية، يعاقب بالحبس من سنة على الأقل إلى خمس سنوات على الأكثر وبغرامة من 500 إلى 20.000د.ج". يراجع: د. أحسن بوسقيعة. الوجيز في القانون الجزائي الخاص. الجزء الأول، دار هومة، الجزائر، ط4. ص303.

[3] اللواء. د. محمد فاروق عبد الحميد كامل. جريمة النصب والاحتيال. الأبعاد القانونية وإجراءات المكافحة. جامعة نايف العربية للعلوم الأمنية. الرياض2006. ص40.

[4] د. محمد فاروق عبد الحميد كامل، المرجع السابق، ص44. ويراجع أيضا: طاهر جليل الحبوش. المرجع السابق. ص26.

[5] *Jean pradel. Michel danti –Juan. Droit pénal spécial. 3eme édition. 2004. Rue de la maison blanche. Paris. P610.*

ولا يشترط لقيام جريمة النصب، حسب الرأي الراجح فقها وقضاء، توافر الضرر،[1] لأن الحكمة من تجريم النصب هي حماية الملكية وحماية الإرادة وسلامتها في التصرف، وإقدامُ شخص على الاحتيال قرينة قاطعة على خطورته الإجرامية التي لا ينال منها عدمُ تحقق الضرر، ويتضح ذلك جليا من تطبيقات القضاء الفرنسي الذي يعتبر أن النصب هو الاحتيال للاستيلاء على جزء أو كل ثروة الغير، وأن الضرر ليس ضروريا لقيام الجريمة، إذ يكفي مجرد تسليم المال، رغم أنه يبدو للوهلة الأولى أن المادة 1/313 ق ع ف، والتي عوضت المادة 405، تشترط الضرر، إلا أنه يمكن الرد: أن مجرد حرمان الضحية من إرادته الحرة يشكل ضررا؛[2] فقد قضت محكمة النقض الفرنسية بالاكتفاء بالضرر المعنوي، وهو المساس بإرادة المجني عليه في التصرف في ماله بصفة صحيحة، إذا تم تسليم المال بناء على الاحتيال، ولو لم يترتب عن ذلك انتقاص لثروة المجني عليه، ولذلك تقوم جريمة النصب بوقوع أي ضرر ولو كان محتملا، طالما توافرت نية الاحتيال.[3]

غير أنه يجب لقيام جريمة النصب، توافر العلاقة السببية بين السلوك الإجرامي والنتيجة، فإذا لم يؤد الكذب عبر الانترنت مثلا إلى دفع الجمهور إلى التعاقد، انقطعت العلاقة السببية، وبالتالي لا تقوم جريمة النصب، بيد أن هذا النشر الكاذب عبر الانترنت أو غيرها يشكل في حد ذاته خطورة كبيرة، مما دفع الكثير من التشريعات إلى تجريمه بنصوص خاصة.[4]

ثانيا: النصب في مجال التجارة الإلكترونية.

يقصد بالنصب أو الاحتيال في مجال التجارة الإلكترونية، كل سلوك خداعي مرتبط بالحاسب الآلي، يهدف الشخص بواسطته إلى الحصول على فائدة أو مصلحة مادية، ومن الصور المنتشرة له استغلال مواقع الانترنت للاحتيال على الغير، عبر مشاريع وهمية، أو من خلال الوصول إلى أرقام بطاقات ائتمان العملاء، واستغلالها في عمليات شراء أو دفع غير مشروعة، وأنشطة التلاعب بالأسهم المالية، وإدارة المحافظ الإلكترونية، ومزادات البضائع على الانترنت... وما من شك

---

[1] إلا أن هناك من يرى ـ حسب نص المادة 372 "التوصل أو محاولة التوصل إلى استلام كل أو بعض مال الغير" أن جريمة النصب تفترض ضررا يتمثل في استلام بعض أو كل مال الغير، وعليه لا تقوم جريمة النصب إذا كان المال ملكا للجاني وتوصل إلى استرجاعه من غيره بطرق احتيالية. يراجع: د. دردوس مكي، القانون الجنائي الخاص في التشريع الجزائري، الجزء الأول، ديوان المطبوعات الجامعية، الجزائر 2005، ص41.

[2] *Jean pradel. Michel danti –Juan.opcit. p609.*

[3] د. أبو الوفا، المرجع السابق، ص46.

[4] د. أبو الوفا، المرجع السابق، ص49.

أن هذه الأنشطة غير المشروعة تهدد كل المتعاملين عبر الوسائل الإلكترونية وخاصة الانترنت سواء أكانوا أفرادا أم شركات، وتقوض ثقة العملاء في التجارة الإلكترونية.[1]

من خلال استقراء النصوص التشريعية المتعلقة بالنصب في كل من الجزائر وفرنسا ومصر وبعض الدول العربية، يمكننا القول بأن صور هذه الجريمة، والتي تشكل ركنها المادي، تتمثل إجمالا في:

- استعمال طرق احتيالية.
- اتخاذ اسم كاذب أو صفة غير صحيحة.
- تقرير أمر كاذب عن واقعة معينة.[2]

من صور النصب أيضا في مجال التجارة الإلكترونية، الإيهام بوجود مشروع كاذب، وقد استقرت أحكام القضاء الفرنسي على أن نشر معلومات كاذبة في الصحف وغيرها من وسائل الإعلام، يعد من الوسائل الاحتيالية التي تقوم بها جريمة النصب، إذا أو هِم المجني عليهم بمشروع كاذب أو بُعث فيهم الأمل في تحقيق ربح وهمي.

والمشروع الكاذب أو الوهمي هو الذي ليس له في الحقيقة وجود، بل مجرد ستار للاستيلاء على أموال الغير.[3]

ولا يشترط لوقوع الاحتيال أن يكون المشروع كله وهميا، تطبيقا لما هو مقرر في جريمة النصب التي تقوم حتى إذا تعلق الكذب ببعض جزئياتها التي تهم المجني عليه.

وتقوم الجريمة إذا قام أحدهم بدعوة الغير عن طريق النشر عبر الانترنت وغيرها –إذ لا تهم وسيلة دعوة الغير– إلى المساهمة في شركة مدعيا أنها تحقق أرباحا طائلة، متى أصبحت هذه الشركة لا تحقق هذه الأرباح، حتى وإن كانت تحققها فيما مضى.[4]

وقد قضت محكمة النقض المصرية، بوقوع جريمة النصب، حتى وإن كان في قدرة الجاني القيام بما وعد به، طالما أن نيته الأولى كانت تهدف إلى مجرد الاستيلاء على المال دون تحقيق المشروع

---

[1] د محمود أحمد طه، المرجع السابق، ص144.

[2] الفريق. طاهر جليل الحبوش، المرجع السابق، ص31.

[3] د أبو الوفا، المرجع السابق، ص50.

[4] المرجع نفسه، ص51.

الموعود به،[1] والدعاية المولدة للأمل في ربح وهمي، عن طريق النشر في وسائل الإعلام المختلفة ومن بينها الوسائل الالكترونية كالانترنت، لأن النشر يدعم المزاعم الكاذبة حول الناشر الذي قد يكون شركة مساهمة تريد بيع أسهمها، ويؤثر على المكتتبين، فمتى تحققت النتيجة وهي إقدام الغير على الاكتتاب بعد أن حذاهم الأمل في الحصول على ربح ليس له من الحقيقة شيء، أو كانت نسبة الحقيقة فيه يسيرة، قامت جريمة النصب.

والربح الوهمي يشمل الربح المادي والمعنوي، ويعتبر الربح وهميا ولو كان هناك أمل في تحقيقه، أو كان لادعاء الجاني نصيب من الحقيقة، ولكن لا يبرر الربح الذي يدّعيه.[2]

ومن صور النصب في مجال التجارة الإلكترونية أيضا الغش باتخاذ اسم كاذب أو صفة غير صحيحة، إذ يكفي لقيام جريمة النصب أن يتخذ الجاني اسما كاذبا أو صفة غير صحيحة، حتى ولو لم يتم استعمال طرق احتيالية أخرى، والهدف من وراء ذلك الحصول على منافع اقتصادية كحيازة مال أو تحويله أو استخدامه عن طريق وثائق تخص الغير، أو التلاعب في البيانات المدخلة والمخزنة بالحاسب الآلي عن طريق شخص يستخدمه باسمه أو باسم شركائه في سبيل استخراج شيكات أو فواتير غير مستحقة، [3]وينطبق هذا الأمر أيضا على المسؤولين عن شركات المساهمة إذا أوردوا أسماء للغير كذبا في نشرات الاكتتاب أو إعلاناتها، باعتبارهم أعضاء مؤسسين فيها، ذلك أن الناس تثق عادة بمثل هذه الأسماء، خاصة إذا كانت من الشخصيات البارزة والمرموقة في المجتمع.[4]

فإذا اعتقد المجني عليه بأن أشخاصا ما لهم صفة معينة فسلم المال بناء على وهمه هذا، فلا تقوم جريمة النصب.[5]

---

[1] المرجع نفسه، ص52.

[2] قضت محكمة النقض المصرية بأن الأمل في الربح يعتبر وهميا، حتى ولو قام هذا الأمل بالفعل، ولكن تحققه يقتضي إنفاق مبالغ تفوق بكثير المبلغ الذي يزعمه المتهم. انظر المرجع السابق. ص57.

[3] بوقرين عبد الحليم، المرجع السابق، ص577.

[4] د. أبو الوفا، المرجع السابق، ص60.

[5] تطبيقا لهذا قضت محكمة التمييز الأردنية بأنه يلزم ادعاء الجاني صفة غير صحيحة ونسبتها إليه، أما لو اتخذ موقفا سلبيا بأن ترك الغير يعتقد في صفة ليست له، واستطاع الحصول بذلك على مبلغ من المال، فلا يتوافر ركن الاحتيال، ويكون من سلم المال قد فرط في حق نفسه. المرجع نفسه، ص60.

وتقع جريمة النصب أيضا في حق من يدعي صفة معينة،[1] كأن يدعي أحد الأشخاص أنه مؤسس شركة أو مديرها، أو عضو مجلس إدارتها، فيؤدي ذلك إلى دفع الجمهور إلى الاكتتاب في هذه الشركة، حتى ولو كانت حقيقية.[2]

وتقوم جريمة النصب أيضا بإساءة الجاني لصفته الحقيقية، بإضافة عناصر أو سلطات أو مزايا إليها، وهي في الحقيقة غير متوفرة فيها، لحمل الناس على تسليمه المال، حيث تتوافر هنا الطرق الاحتيالية في حقه، إذ اعتمد على المظهر الخارجي الذي يبعث الغير على تصديقه نظرا لصحة الصفة التي يتحلى بها،وهذا ما أخذت به صراحة المادة 1/313[3] ق.ع.ف، ويتبناه القضاء في كل من فرنسا ومصر.[4]

وفيما يخص التجارة الإلكترونية، فإن التساؤل التالي يطرح نفسه: **إلى أي مدى يجوز إعمال نصوص النصب في مجال التجارة الإلكترونية؟**

فيما يخص محل جريمة "النصب المعلوماتي"، فإنها تتشابه مع جريمة "السرقة المعلوماتية[5]" لذلك ما قيل حول هذا المحل عند التطرق لجريمة السرقة هو ذاته ما يقال عن جريمة النصب في مجال التجارة الإلكترونية، يضاف إلى ذلك أن المشرع الفرنسي في م313-1 ق ع ف نص على أن محل النصب يمكن أن يكون قيمة أو مالا أو خدمة أو عملا ينتج عنه التزام أو تحرر من التزام، بمعنى أن المشرع الفرنسي جعل الخدمات مساوية للمال، واستعمل أيضا مصطلح قيمة، وكأنه يرغب في اعتبار القيمة المعنوية محلا لجريمة النصب لأن الأشياء ذات القيمة المادية تدخل في نطاق الأموال، وبناء عليه

---

[1] لم تعرف محكمة النقض المصرية الصفة غير الصحيحة، واكتفت بإيراد أمثلة لها، ومنها انتحال لقب أو وظيفة أو مهنة أو قرابة أو ما شاكل ذلك. يراجع: المرجع نفسه، ص61.

[2] المرجع نفسه، ص60.

[3] تنص المادة 1/313 ق ع ف على:

"L'escroquerie est le fait, soit par l'usage d'un faux nom ou d'une fausse qualité, soit par l'abus d'une qualité vraie, soit par l'emploi de manoeuvres frauduleuses, de tromper une personne physique ou morale et de la déterminer ainsi, à son préjudice ou au préjudice d'un tiers, à remettre des fonds, des valeurs ou un bien quelconque, à fournir un service ou à consentir un acte opérant obligation ou décharge.
L'escroquerie est punie de cinq ans d'emprisonnement et de 375000 euros d'amende".

[4] د. أبو الوفا. المرجع السابق. ص62.

[5] د. عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية، منشأة المعارف، الإسكندرية، مصر (دون ذكر سنة النشر). ص143.

تقوم جريمة النصب إذا تمكن الجاني بطرق احتيالية من حمل المجني عليه على تسليم لعبة إلكترونية أو سيناريو أو قصة، سواء أكانت مثبتة في منقول أم لا.[1]

طرح الفقه أيضا التساؤل التالي: **ما مدى إمكانية الاحتيال على الحاسب الآلي؟**

انقسم الفقه حول هذه المسألة إلى ثلاثة اتجاهات؛[2] اتجاه يرى عدم إمكانية وقوع فعل الاحتيال على الحاسب، حيث يجب أن يكون طرفا جريمة النصب أشخاصا طبيعيين، ولا يتصور هنا إلا إذا تم خداع الشخص المكلف بالبيانات، واتجاه ثان يرى إمكانية وقوع فعل الاحتيال على الحاسب، ويمثل هذا الاتجاه تشريعات الدول الأنجلوسكسونية، وتشريعات بعض دول الولايات المتحدة الأمريكية، وبعض الفقه الفرنسي، ويستند هذا الأخير إلى حكم محكمة النقض الفرنسية بتطبيق عقوبة النصب على شخص وضع قطعا معدنية عوض قطع النقود للاحتيال على عداد أماكن الانتظار، وترتب عن ذلك خداع الآلة، مما جعل المحكمة تعتبر هذا الفعل من قبيل الطرق الاحتيالية الذي تقوم به جريمة النصب، كما أن جانبا من الفقه المصري يرى أن غش العدادات والأجهزة الحسابية نوع من الكذب الذي تتحقق به الطرق الاحتيالية. أما الاتجاه الثالث فيمثله التشريع الأمريكي وبعض الفقه الفرنسي، حيث تطبق النصوص المتعلقة بالغش في مجال البنوك والبريد والتلغراف...

ويرى جانب من الفقه جواز تطبيق نصوص النصب على المعاملات الإلكترونية بشروط، هي الاستيلاء على مال الغير، استخدام الحاسب الآلي أو الوسيلة الإلكترونية بصفة عامة، والتدخل مباشرة في المعطيات بإدخال معلومات وهمية، أو تعديل البرامج أو إنشاء برامج صورية، ويستوي حسب محكمة النقض الفرنسية أن يكون التسليم في جريمة النصب المعلوماتي ماديا أو ما يعادله،[3] وهو ما اصطلح عليه فيما بعد بالقيد الكتابي، وبهذا الحكم تكون المحكمة قد أخذت بعين الاعتبار كل

---

[1] بيومي حجازي، المرجع السابق، ص215، ويراجع أيضا: طعباش أمين، الحماية الجنائية للمعاملات الإلكترونية، مذكرة ماجستير في العلوم القانونية تخصص علم الإجرام والعقاب، جامعة الحاج لخضر باتنة، 2013/2012، ص104.

[2] يراجع كل من:

- عبد الحليم بوقرين، المرجع السابق، ص178.
- عفيفي كامل عفيفي، المرجع السابق، ص150 وما بعدها.
- محمد عبيد الكعبي، المرجع السابق، ص466 وما بعدها.
- بيومي حجازي، المرجع السابق، ص216 وما بعدها.

[3] محمد عبيد الكعبي، المرجع نفسه، ص468.

أشكال النقود، بما فيها النقود الإلكترونية وغيرها من وسائل الدفع الإلكترونية، والتي تعد الوسيلة الأكثر شيوعا في مجال التجارة الإلكترونية.[1]

والجدير ذكره أن بعض التشريعات ومنها التشريع الألماني والياباني لا تعتبر وسائل الدفع الكتابية أموالا، بل ديونا، ولذلك لا تجعلها محلا لجريمة النصب، على خلاف ما حكمت به محكمة النقض الفرنسية، وما هو معمول به في تشريعات دول أخرى كالولايات المتحدة الأمريكية وسويسرا وانجلترا. [2]

كما أن الفقه الفرنسي ابتكر نظرية "التسليم المعادل" لمواجهة حالات الاحتيال الواقع باستعمال الحاسب الآلي، خاصة على ضريبة المبيعات، وعدادات موقف انتظار السيارات والهواتف، ومفادها أن الدفع يتم بواسطة القيد كتابة، وهو ما يعادل التسليم المادي للأموال.[3]

في القانون الجزائري وبالرجوع إلى نص م372 ق ع المتعلقة بجريمة النصب، نجد أنها لا تعير اهتماما للوسيلة التي تم بها الحصول على مال الغير ما دامت هناك طرق احتيالية، كما أنها لا تركز على المجني عليه بل على الجاني، مما يدفع إلى القول بجواز إعمال نص هذه المادة لحماية أموال التجارة الإلكترونية. رغم ذلك يرى البعض أن صياغة نص المادة 1/313 ق ع ف أفضل من صياغة المشرعين الجزائري والمصري لاشتمالها على الأموال المعنوية.

والجدير ذكره ما نص عليه المشرع الإماراتي في القانون التجاري رقم 02 لسنة 2006 المتعلق بمكافحة جرائم تقنية المعلومات، حيث نص صراحة على جريمة النصب الإلكتروني في م10 منه، وتجنب النص الحديث عن خداع المجني عليه، ولم يستلزم تسليم الأموال للجاني، كما نصت اتفاقية بودابست الأوربية للإجرام المعلوماتي في م8 على جريمة النصب الإلكتروني، ودعت الدول الأعضاء إلى تبني ما جاء فيها في قوانينها الداخلية.[4]

[1] بوقرين عبد الحليم، المرجع السابق، ص180.

[2] طعباش أمين، المرجع السابق، ص113.

[3] أمال قارة، المرجع السابق، ص49.

[4] محمد عبيد الكعبي، المرجع السابق، ص473.

جريمة النصب المعلوماتي جريمة عمدية تتطلب لقيامها توافر القصد الجنائي العام بعنصريه العلم والإرادة، بالإضافة إلى القصد الخاص، وهو نية التملك أي الاستيلاء على مال مملوك للغير، ويقوم القصد الخاص في الفرض الذي يستخدم فيه الجاني بطاقة ائتمان مثلا، وهو يعلم أن رصيده ليس به ما يكفي، أو أن بطاقته منتهية أو موقوفة، ويستخدمها رغم ذلك في الحصول على سلع أو خدمات، مع علمه أنه لا حق له في ذلك.[1]

الفرع الثالث: جريمة التزوير.

نتعرض أولا إلى مفهوم جريمة التزوير بصفة عامة، ثم نحاول أن نرى إلى أي مدى يجوز أن تمتد الحماية المقررة للأموال وفق نصوص جريمة التزوير إلى معاملات التجارة الإلكترونية.

أولا: مفهوم جريمة التزوير.

تعتبر جرائم التزوير بمختلف أنواعها[2] جرائم مخلة بالثقة، فهي تقوم على تغيير الحقيقة،[3] لذلك يعرف التزوير بأنه تغيير الحقيقة في بيانات محرر ما بإحدى الطرق المحددة، مع ترتب ضرر للغير، ومع نية استعمال المحرر فيما زُور من أجله،[4] أو هو تغيير الحقيقة بقصد الغش في محرر بإحدى الطرق المقررة قانونا، تغييرا من شأنه أن يسبب ضررا للغير،[5] أو هو باختصار إظهار الكذب في محرر بمظهر الحقيقة غشا لعقيدة الغير.[6] وقد اعتبرت المادة 214 ق ع بأنه يعتبر مرتكبا لجريمة التزوير كل موظف أو قائم بوظيفة عمومية أو قاض،[7] يغير في حقيقة المحررات العمومية أو الرسمية أثناء تأدية وظيفته وذلك بوضع توقيعات مزورة، أو إحداث تغيير في المحررات أو الخطوط أو التوقيعات، أو انتحال شخصية الغير أو الحلول محلها، أو الكتابة في السجلات أو غيرها من المحررات العمومية، أو

---

[1] المرجع نفسه، ص472.

[2] وردت جرائم التزوير بأنواعها في المواد من: 197 إلى 241 ق ع، مقسمة إلى أربع مجموعات، وهي: تزوير النقود وما يتصل بها، تقليد أختام الدولة والطوابع والعلامات، التزوير في المحررات، وشهادة الزور وما شابهها. انظر: د. أحسن بوسقيعة، الوجيز في القانون الجزائي الخاص، الجزء الثاني. ط3، دار هومة، الجزائر 2006، ص307.

[3] د أحسن بوسقيعة، المرجع السابق، ص307.

[4] فهد بن محمد النفيعي، الحماية الجنائية للسوق المالي السعودي، رسالة دكتوراه في فلسفة العلوم الأمنية، جامعة نايف العربية للعلوم الأمنية، الرياض 2006، ص200.

[5] د. أبو الوفا، المرجع السابق، ص57.

[6] د. رمسيس بهنام، قانون العقوبات، جرائم القسم الخاص، منشأة المعارف، الإسكندرية، مصر، دون ذكر سنة النشر، ص 437.

[7] كما يجوز أن يرتكب جريمة التزوير غير الموظف كما نصت على ذلك المادة 216 ق ع.

التغيير فيها بعد إتمامها وقفلها. ولكن هذه المادة قد لا تطبق على المتعاملين عبر شبكة الانترنت[1] لاعتبارين اثنين، أولهما صفة الجاني والتي تفترض أن يكون موظفا عاما أو قاضيا أو قائما بوظيفة عمومية، وثانيهما لأن التزوير يجب أن ينصب على محرر عمومي أو رسمي، ولكن يجوز إعمال نص م219 ق ع التي تعاقب على التزوير في المحررات العرفية أو التجارية أو المصرفية من طرف أي شخص.

ولجريمة التزوير في المحررات، ركنان: ركن مادي يتمثل في تغيير الحقيقة في محرر بإحدى الطرق المنصوص عليها قانونا، تغييرا من شأنه إحداث ضرر؛ وركن معنوي يتمثل في القصد الجنائي.[2]

فأما الركن المادي فيتناول محل الجريمة وهو المحرر،[3] وتغيير الحقيقة،[4] وطرق التزوير،[5] والضرر.[6]

وأما الركن المعنوي فيلزم لتوافره كلاّ من القصد العام،[7] والقصد الخاص.[1]

---

[1] غير أنه بالإمكان إعمالها عند تطبيق الحكومة الإلكترونية.

[2] أحمد أبو الروس، جرائم التزييف والتزوير والرشوة واختلاس المال العام من الوجهة القانونية والفنية، المكتب الجامعي الحديث، الأزاريطة، الإسكندرية، بدون سنة نشر. ص61.

[3] يلزم للمحرر أن يتخذ شكل الكتابة، بأي خط دونت، وبأي لغت كتبت، وبصرف النظر عمن دوّنها، وعن المادة التي كتبت عليها. ويلزم أن يكون مصدر المحرر ظاهرا فيه، كما يجب للمحرر أن يتضمن تعبيرا متكاملا عن مجموعة من المعاني والأفكار المترابطة فيما بينها. انظر المرجع نفسه، ص62 وما بعدها. وقد أضاف المشرع الفرنسي عبارة "كل سند آخر للتعبير عن الفكر" إلى المحرر ليتسع مدلوله إلى أشرطة التسجيل والأقراص المغنطة وغيرها لمواكبة التطورات التكنولوجية الحديثة. انظر: د. أحسن بوسقيعة. المرجع السابق. ص336. وانظر أيضا:

Jean f et Michel d. op cit. p790.

وتنص المادة 1/414 ق ع ف:

"Constitue un faux toute altération frauduleuse de la vérité, de nature à causer un préjudice et accomplie par quelque moyen que ce soit, dans un écrit ou tout autre support d'expression de la pensée qui a pour objet ou qui peut avoir pour effet d'établir la preuve d'un droit ou d'un fait ayant des conséquences juridiques.
Le faux et l'usage de faux sont punis de trois ans d'emprisonnement et de 45000 euros d'amende".

[4] تغيير الحقيقة هو الفعل الإجرامي الذي يقوم به التزوير، ويعني إبدالها بما يغايرها، ويكفي أن يمس التغيير بيانا واحدا من المحرر. والمراد بالحقيقة ما يتعين إثباته في المحرر من قبل صاحب الشأن، وفق ما يقرره القانون. يراجع: أبو الروس. المرجع السابق. ص64 وما بعدها.

[5] اشترط المشرع أن يقع التزوير بطرق معينة وردت على سبيل الحصر. ويمكن تقسيمها إلى طرق مادية، وطرق معنوية، فالطرق المادية هي: 1- وضع إمضاءات أو أختام أو بصمات مزورة، 2- تغيير المحررات أو الأختام أو الإمضاءات أو زيادة الكلمات، 3- وضع أسماء أو صور أشخاص آخرين مزورة، 4- التقليد، 5- الاصطناع وهو إنشاء محرر بكامل أجزائه على شاكلة أصل موجود، أو إنشاء محرر على غير مثال سابق. أما طرق التزوير المعنوي فقد حددها المشرع المصري في ثلاث: 1- تغيير إقرار أُولي الشأن الذي كان الغرض من تحرير السندات إدراجه بها، 2- جعل واقعة مزورة في صورة واقعة صحيحة، 3- جعل واقعة غير معترف بها في صورة واقعة معترف بها. لمزيد من التفصيل يراجع: أبو الروس المرجع السابق. ص66 وما بعدها.

[6] ويشترطه الفقه والقضاء، وهو غير مندمج في القصد الجنائي، ومميز عنه، فهو ذلك الفعل المادي المنتهي إلى العالم الخارجي، وقد يكون الضرر ماديا أو معنويا، محققا وحالا أو محتملا، فرديا أو اجتماعيا. أبو الروس. المرجع السابق. ص73 وما بعدها.

[7] والمتمثل في إرادة النشاط مع العلم بكافة عناصر الركن المادي للجريمة.

ويعد الغش المدعوم بالتزوير نوعا من الطرق الاحتيالية الذي تقوم به جريمة التزوير وجريمة النصب أيضا، ويُحكم بعقوبة الجريمة الأشد على المرتكبين.[2]

ثانيا: جريمة التزوير والتجارة الإلكترونية.

التساؤل المطروح دوما هو: مدى انطباق أركان جريمة التزوير التقليدية على التزوير في مجال التجارة الإلكترونية بصفة خاصة، والتزوير المعلوماتي عامة؟

التزوير المعلوماتي هو التزوير الذي يتم بوسيلة معلوماتية في محرر معلوماتي، أو بوسيلة إلكترونية في محرر إلكتروني، ضمن إطار الجريمة المعلوماتية.[3]

يتعين علينا إذن الإجابة عن السؤال التالي: ما المقصود بالمحرر الإلكتروني؟

عرف المشرع المصري في القانون رقم 15 لسنة 2004 والمتعلق بالتوقيع الإلكتروني في م1/ب المحرر الإلكتروني بأنه: "رسالة تنشأ أو تدمج أو تخزن أو ترسل أو تستقبل كليا أو جزئيا بوسيلة إلكترونية أو رقمية أو ضوئية أو بأية وسيلة أخرى مشابهة" واستعملت دول أخرى مصطلحات مترادفة منها المستند الإلكتروني والوثيقة الإلكترونية،[4] وقد عرفه قانون المعاملات الالكترونية لإمارة دبي بأنه: "سجل أو مستند إلكتروني يتم إنشاؤه أو تخزينه أو استخراجه أو نسخه أو إرساله أو إبلاغه أو استلامه بوسيلة إلكترونية، على وسيط ملموس أو على وسيط إلكتروني آخر، ويكون قابلا للاسترجاع بشكل يمكن فهمه"، كما أن قانون الأونسترال عرف المحرر الإلكتروني وهو يشمل المحررات التي يتم تخزينها في الحاسب الآلي أو على شبكة الانترنت أو أي وسيط إلكتروني.[5]

---

[1] وهو اتجاه نية المزور لحظة ارتكاب فعل تغيير الحقيقة إلى استعمال المحرر المزور فيما زُوّر من أجله، حتى ولو لم يستعمل المحرر المزور فيما بعد. يراجع: أبو الروس. المرجع السابق. ص78.

[2] د. أبو الوفا، المرجع السابق. ص57.

[3] المستشار الدكتور خالد محمد كدفوري المهيري، جرائم الكمبيوتر والإنترنت والتجارة الإلكترونية، دار الغرير للطباعة والنشر، دبي، الإمارات العربية المتحدة، دون ذكر سنة النشر، ص634.

[4] د. إيهاب فوزي السقا، جريمة التزوير في المحررات الإلكترونية، دار الجامعة الجديدة، الإسكندرية، مصر 2008، ص14.

[5] د. محمد فواز المطالقة، الوجيز في عقود التجارة الالكترونية، دراسة مقارنة، الطبعة الأولى، الإصدار الثاني، دار الثقافة للنشر والتوزيع، عمان، الأردن 2008.

أما في المجال الفقهي فقد حاول الفقه إعطاء تعريفات للمحرر الإلكتروني، ومنها: "هو كل جسم منفصل أو يمكن فصله عن نظام المعالجة الآلية للمعطيات، أو يكون مشتقا من هذا النوع". وعليه فإن المحرر الإلكتروني هو المحرر الذي يتضمن بيانات معالجة إلكترونيا، ومكتوب وموقع عليه بطريقة إلكترونية، وموضوع على دعامة مادية، مع إمكانية تحويله إلى محرر ورقي عن طريق إخراجه من مخرجات الحاسب الآلي،[1] لذا يتميز المحرر الإلكتروني بمجموعة من الخصائص منها:[2]

– المحرر الإلكتروني يتضمن تعبيرا عن المعاني والأفكار الإنسانية، لها قيمة يعول عليها عند المعاملات بين الأفراد والمؤسسات والحكومات، ويترتب عن تغيير ما يحمله من حقائق مساءلات قانونية.

– يحمل هذا المحرر الصفة الإلكترونية، مما يعني أن مختلف العمليات التي يمر بها متصلة بتقنية تكنولوجية إلكترونية أو رقمية، ولا يمكن استخدامه خارج الوسيط الإلكتروني أو الرقمي.

– يمكن تحميل هذا المحرر ونقله من جهاز إلى آخر عن طريق دعامة إلكترونية.

– يحمل هذا المحرر– ما دام على الوسيط الإلكتروني – الطابع المعنوي للأشياء.

– يتم إرسال هذا المحرر عبر شبكات وأجهزة الحاسب الآلي من جهاز إلى آخر عن طريق تحويله إلى رموز أو نبضات... ثم تحويله إلى كلمات مفهومة عن طريق بروتوكولات التعامل عبر الأجهزة الإلكترونية.

– يمكن إرسال أو استقبال هذا المحرر إلى أي مكان في العالم في الوقت نفسه.

من أسباب ظهور المحرر الإلكتروني، ازدهار التجارة الإلكترونية، إذ أن قوام هذه التجارة تبادل السلع والخدمات، و لا يتأتى ذلك إلا عن طريق عقد يستجمع الشروط القانونية بين أطرافه ليرتب آثارا قانونية، وهذا العقد يكتب إلكترونيا تتوافر فيه كل أركان وشروط العقد المكتوب (التقليدي)، ويذيل بتوقيع إلكتروني يتناسب مع طبيعته.[3]

ولا بد من توثيق المحرر الإلكتروني أيضا لدى جهة معتمدة يتم تحديدها من قبل الحكومة، يكون عمل هذه الجهة التحقق من صحة المحرر الذي تم إصداره، ومن شخصية مصدره،

[1] السقا، المرجع السابق، ص16.

[2] المرجع نفسه، ص17.

[3] المرجع نفسه، ص22.

ومنح صاحب المحرر شهادة التوثيق التي تؤكد صحة المحرر الإلكتروني، ويتم منح صاحب المحرر رمز تعريف شخصي خاص به، ليميز المحرر عن غيره من المحررات الإلكترونية تجنبا للخلط بينها.[1]

كانت م5/462 ق ع ف قبل إلغائها تنص على معاقبة من يقوم عمدا بتغيير للحقيقة في المحررات المعالجة آليا أيا كان شكلها إذا ترتب عن ذلك ضرر، وعلى معاقبة من يستعمل هذه المحررات المزورة.

الملفت للانتباه بخصوص هذه المادة هو محل تغيير الحقيقة، أي المحرر الإلكتروني المعالج آليا، وعليه يخرج من نطاق الجريمة المستندات أو المحررات غير المعالجة آليا ولو كانت محررات إلكترونية، كالبطاقات البنكية التي لم تدخل الخدمة بعد، وتذاكر المترو، والأوراق المعدة لتسطير المعلومات عليها.[2] فالمشرع الفرنسي في هذه المادة قبل إلغائها قصر جريمة التزوير على المحرر الذي يتخذ شكل الكتابة لأنها تصلح لنقل المعنى من شخص إلى آخر، واستبعد الأسطوانات وأشرطة التسجيل وغيرها من الدعامات التي لا تتخذ شكل الكتابة.[3]

وقد كان فريق من الفقه الفرنسي يذهب إلى إمكانية تطبيق نصوص التزوير التقليدية على التزوير المعلوماتي، لأن الكتابة وإن كانت مطلبا رئيسا في جرائم تزوير المحررات إلا أنه ينبغي تغليب روح النص على الألفاظ، واعتبار ما يظهر على شاشة الحاسب الآلي شكلا مستحدثا للمحرر، كما أن القضاء لا يفرق بين محرر منسوخ أو مشفر.[4] إلا أن المشرع الفرنسي قد حسم الأمر في م1/414 ق ع ف لسنة 1992 (الذي دخل حيز التنفيذ سنة 1994) التي ألغت م 5/462 والتي وسعت من مفهوم المحرر الذي يمكن أن يقع عليه التزوير ليشمل كل وسيط آخر للتعبير عن الأفكار، وهذا لا ينطبق فقط على المحررات المعالجة آليا، بل يشمل أيضا البرامج أيا كان نوعها، والمعلومات المسجلة على أقراص أو شرائط ممغنطة ولم تتم معالجتها بعد أو إدخالها إلى الحاسب الآلي،

[1] فواز المطالقة، المرجع السابق، ص209.

[2] القهوجي، المرجع السابق، ص140.

[3] المرجع نفسه، ص144.

[4] نهلا عبد القادر المومني، المرجع السابق، ص150.

والتعليمات المتعلقة بكيفية تشغيل البرامج، وتذاكر المترو وبطاقات الائتمان وبطاقات الدفع والسحب حتى ولو لم تدخل الخدمة بعد.[1]

ويرى البعض أن المشرع الفرنسي قد حقق من وراء هذا التعديل هدفين مهمين:[2] الأول اتساعه ليشمل التزوير التقليدي والتزوير المعلوماتي، والثاني خروج جريمتا تزوير المحررات المعالجة آليا واستعمالها من بين جرائم الاعتداء على نظام المعالجة الآلية للمعطيات، لاختلاف المصلحة المحمية قانونا، إذ أن هذه المصلحة في جرائم الاعتداء على نظام المعالجة الآلية للمعطيات، مصلحة فردية تخص صاحب نظام المعلوماتي فردا أو مؤسسة، أما المصلحة المحمية في جرائم التزوير فهي حماية الثقة العامة في هذه المحررات أيا كان شكلها.

أما طرق التزوير في المحررات الإلكترونية، فإنها تكون من قبيل الطرق المادية وليس المعنوية، وهي التقليد والتوقيع والحذف والإضافة والتعديل أو التغيير.[3] ولم يهتم المشرع الفرنسي بالوسيلة التي يتم تغيير الحقيقة بها، فلم يحصر الطرق التي تقع بها جريمة التزوير على خلاف المشرع المصري في م424 ق ع م،[4] وكذا المشرع الجزائري في م219 ق ع، وعليه ندعو مشرعنا أن يحذو حذو نظيره الفرنسي ويوسع في طرق التزوير، بحيث لا يحصرها كي تستطيع مسايرة الأحداث المتغيرة باستمرار، وكذا يوسع في المحل الذي يقع عليه التزوير بحيث يشمل المحرر التقليدي وأي محرر آخر للفكر مهما كانت طبيعته، أسوة بنظيره الفرنسي.

الفرع الرابع:جريمة خيانة الأمانة.

نتعرض أولا إلى مفهوم جريمة خيانة الأمانة بصفة عامة، ثم نحاول أن نرى إلى أي مدى يجوز أن تمتد الحماية المقررة للأموال وفق نصوص جريمة خيانة الأمانة إلى معاملات التجارة الإلكترونية.

---

[1] القهوجي، المرجع السابق، ص145.

[2] بيومي حجازي، التزوير في جرائم الكمبيوتر والانترنت، دار الكتب القانونية، المحلة الكبرى، مصر 2008، ص161 وما بعدها.

[3] القهوجي، المرجع السابق، ص145.

[4] بيومي، المرجع السابق، ص163.

أولا: مفهوم جريمة خيانة الأمانة.

تُعرّف خيانة الأمانة بأنها اختلاس أو استعمال أو تبديد مال منقول مملوك للغير، سُلّم إلى الجاني بناء على عقد من عقود الأمانة المحددة حصرا في القانون، إضرارا بمالكه أو صاحبه أو واضع اليد عليه، مع توافر القصد الجنائي.[1]

وقد تطرق المشرع الجزائري إلى خيانة الأمانة في المادة 376 ق ع،[2] واستخدم مصطلح "اختلاس أو تبديد" للتعبير عن الفعل المادي للجريمة، أما المشرع المصري فأضاف مصطلح الاستعمال، ونص المشرع الفرنسي على جريمة خيانة الأمانة في المواد من 314-1[3] إلى 314-4 عقوبات فرنسي.

ومن خلال نص المادة 376 ق ع يمكننا القول بأن الجريمة تتكون من ركنين: مادي ومعنوي؛ فأما الركن المادي فيتمثل في اختلاس الجاني أو تبديده محل الجريمة، المتمثل في مال منقول، مسلّم له بناء على عقد من عقود الأمانة، مما قد يضر بمالك الشيء أو صاحبه أو واضع اليد عليه. وأما الركن المعنوي فيتخذ صورة القصد الجنائي، والمتمثل في القصد العام بعنصريه العلم والإرادة، والقصد الخاص والمتمثل في نية الجاني للتملك، أي لتغيير حيازته من حيازة ناقصة إلى حيازة كاملة، مع إنكار حق صاحب المال.[4]

---

[1] د. فوزية عبد الستار. شرح قانون العقوبات. القسم الخاص. دار النهضة العربية. القاهرة. الطبعة الثالثة 1990. ص935.

[2] وقد أشار المشرع الجزائري تحت عنوان خيانة الأمانة إلى أربع جرائم: خيانة الأمانة بالمفهوم الحرفي والمنصوص عليها في المادة 376، استغلال حاجة القصر (م 380)، خيانة التوقيع على بياض (م381)، واختلاس أوراق قضائية (م382). يراجع: د: دردوس مكي. المرجع السابق. هامش ص45.
ونصت المادة 376 ق ع على ما يلي: "كل من اختلس أو بدد بسوء نية أوراقا تجارية أو نقودا أو بضائع أو أوراقا مالية أو مخالصات أو أية محررات أخرى تتضمن أو تثبت التزاما أو إبراء لم تكن قد سُلمت إليه إلا على سبيل الإجارة أو الوديعة أو الوكالة أو الرهن أو عارية الاستعمال أو لأداء عمل بأجر أو بغير أجر بشرط ردها أو تقديمها أو لاستعمالها أو لاستخدامها في عمل معين وذلك إضرارا بمالكيها أو واضعي اليد عليها أو حائزيها يعد مرتكبا لجريمة خيانة الأمانة..."

[3] تنص المادة 314-4 ق ع ف على:

L'abus de confiance est le fait par une personne de détourner, au préjudice d'autrui, des fonds, des valeurs ou un bien quelconque qui lui ont été remis et qu'elle a acceptés à charge de les rendre, de les représenter ou d'en faire un usage déterminé.
L'abus de confiance est puni de trois ans d'emprisonnement et de 375000 euros d'amende.

[4] د. فوزية عبد الستار، المرجع السابق، ص972.

والملاحظ بالنسبة للمشرع الفرنسي في م1/314 ق ع ف أنه استبعد من السلوك الإجرامي لجريمة خيانة الأمانة فعل التبديد، وفعل الاستعمال[1] أيضا واكتفى بفعل الاختلاس، ولعل ذلك راجع إلى أن فعلي التبديد والاختلاس صورتان للسلوك الإجرامي الناشئ عن قيام الجاني بالتصرف بوصفه صاحب الشيء ويستأثر لنفسه بسلطة قانونية لا تخصه، كما أنه لم يحدد عقودا بعينها بوصفها عقودا للأمانة على خلاف المشرعين الجزائري والمصري، وترك المهمة للقضاء للقول ما إن كان العقد من عقود الأمانة أم لا،[2] وهذا المسلك الموسع يساعد أكثر على إعمال نصوص جريمة خيانة الأمانة على بعض المعاملات الإلكترونية.

ثانيا: جريمة خيانة الأمانة والتجارة الإلكترونية.

من صور خيانة الأمانة في بيئة التجارة الإلكترونية قيام موظف مسؤول عن التحويلات الإلكترونية في مؤسسة مالية بالظهور على أموال أحد العملاء بمظهر المالك، وتصرفه فيها على هذا النحو، وكذا إساءة الجاني للأشياء المسلمة إليه على سبيل الأمانة، وذلك بنسخها، كأن يقوم العامل الذي تسلم البرنامج لمعالجة المعطيات الخاصة بالمشروع الذي يعمل به، بمعالجة مشروع آخر خاص بالغير، وهذا حسب الرأي الراجح فقها الذي يجيز أن يكون محل الجريمة من طبيعة غير مادية، وقد قضي في فرنسا بوجود جريمة خيانة الأمانة، نشأت عن استخدام متعسف في استعمال سلعة في أغراض غير مشترطة في العقد، حيث قام الأمين بتسليم الغير عدة شرائط ممغنطة تحتوي على مجموعة من الأغاني، كي يسجلها ويعيدها بعد ذلك إلى مالكها. وطبق القضاء الفرنسي أيضا نصوص جريمة خيانة الأمانة بشأن ممثل شركة تجارية، احتفظ بعد فصله من الشركة ببطاقة العملاء الخاصة بها. ويرى جانب من الفقه الفرنسي أن اغتصاب جهد الآلة بما فيها الحاسب الآلي يندرج ضمن نصوص جريمة خيانة الأمانة.[3]

ولقيام جريمة خيانة الأمانة حسب المشرعين الجزائري والمصري يلزم وجود عقد من عقود الأمانة، وهي الإيجار أو الوكالة أو العارية...م376 ق ع، وهذه العقود كلها يمكن تصورها في بيئة

---

[1] يقصد بالاستعمال استعمال محل الأمانة، مع بقاء هذا المحل على حاله، وفي مجال التجارة الإلكترونية يكون هذا الاستعمال مثلا عندما يقوم الجاني باستعمال برنامج لمعالجة معطيات في غير الأغراض المخصصة له، أو معالجتها للغير.

[2] بيومي حجازي، التجارة الإلكترونية... المرجع السابق، ص250.

[3] المرجع نفسه، ص248 وما بعدها. ويراجع أيضا: مدحت عبد الحليم رمضان، المرجع السابق، ص154، وكذلك أمال قارة، المرجع السابق، ص56.

التجارة الإلكترونية، كما أن المشرع الجزائري استخدم مصطلح أو أية محررات أخرى، وهو مصطلح واسع يسمح بإدراج المحررات الإلكترونية وغيرها، وإن كنا نرى بأن يحذو المشرع الجزائري هنا أيضا حذو نظيره الفرنسي، سواء من حيث محل الجريمة أو العقود التي تتم بها.

الفرع الخامس: جريمة الإتلاف.

نتعرض أولا إلى أركان جريمة الإتلاف بصفة عامة، ثم نحاول أن نرى إلى أي مدى يجوز أن تمتد الحماية المقررة للأموال وفق نصوص الإتلاف إلى معاملات التجارة الإلكترونية.

أولا: أركان جريمة الإتلاف.

تتكون الجريمة كغيرها من الجرائم من ركنين، مادي ومعنوي، بالإضافة إلى الركن الشرعي.

فالركن المادي جريمة الإتلاف يقوم عموما على محوريين أساسيين هما: فعل الإتلاف ووقوع الضرر.

1- فعل الإتلاف:

مبدأ التشريع في جريمة الإتلاف بشكل عام جاء لجهة بيان نتيجة الفعل لا وسيلة ذلك، ولهذا فلا يقيم المشرع وزنا لطبيعة السلوك وعناصره ووسائله، بل يركز على وقوع الضرر، فطالما لحق بالمال المملوك للغير محل الحماية الجزائية ضرر قامت الجريمة بعناصرها العامة، فالمهم أن يأتي الفاعل سلوكا يشكل تعديا على مال مملوك للغير، بغض النظر عن وسيلته أو حجمه أو طبيعته وهو مفهوم فعل الإتلاف الذي يجب أن يشتمل على العناصر الرئيسة التالية:[1]

- سلوك إيجابي أو سلبي ناتج عن إرادة حرة للفاعل.
- أن يشكل السلوك على الوصف السابق تعديا من قبل الفاعل على صاحب المال موضوع الإتلاف ويشترط في ذلك ألا تكون للفاعل أية حقوق متعلقة بذلك المال وأن تتجه إرادته نحو إيقاع الضرر.

[1] جلال محمد الزعبي، أسامة أحمد المناعسة، جرائم تقنية نظم المعلومات الإلكترونية، دراسة مقارنة، دار الثقافة، عمان، الأردن 2010، ص120.

– أن يؤدي هذا التعدي إنقاص في مكونات المال أو في قيمته أو قيمة أي منها، أو في مدى تأديته لوظائفه التي وجد من أجلها، أو لطريقة استعماله على نحو مخصوص، فإن لم يحدث السلوك أي من تلك الأمور أو أشباهها لم يقع به إتلاف.

والملاحظ على مفهوم التشريع والفقه القانوني لفعل الإتلاف كسلوك جرمي مستوجب المسؤولية أن الحديث دائما عن آثار السلوك لا طبيعته وإن كانت كافة صنوف الأموال التي جاءت النصوص الجزائية السالفة على ذكرها تتعلق بأموال مادية إلا أن ذلك لا يقف أمام إطلاق طبيعة الفعل وعدم حصرها في طبيعة مادية هي الأخرى ولهذا أمكن في ظل هذا المفهوم لفعل الإتلاف تصور جريمة إتلاف إلكترونية وهي التي تقوم على سلوك إتلاف ذو طبيعة معنوية لا مادية.[1]

2- وقوع الضرر:

المحور الثاني في جريمة الإتلاف هو الضرر وهو أثر الفعل، فلا جريمة إتلاف بلا ضرر، حتى مع تحقق السلوك، فالإتلاف من جرائم الضرر لا الخطر، والتي اشترط المشرع لقيامها وقوع نتيجة معنية، وهي هنا كما أسلفنا تحقق الضرر.

حين التحدث عن الضرر ومحل المال المتمتع بالحماية القانونية الجزائية فإن المقصود مشتملات المال وماديته لا حق الملكية فيه.

أما الضرر فهو مفهوم عام يختلف بحسب طبيعة وماهية المال موضوعه، فقد يكون الضرر على شكل إنقاص لبعض أو مكونات الشيء الأساسية، بحيث يؤثر ذلك في المال كوحدة واحدة، وبالتالي تعطيله، كما يمكن أن يكون الضرر على شكل إبطال أداء المال لوظيفته، وحرمان صاحبه من إمكانية الإستفادة من ماله، على نحو ما وجد من أجله، ويمكن أن يكون الإتلاف بصور أخرى لا تقع تحت حصر؛ والظاهر أن الإتلاف لا يتحقق إلا بوجود أثر سلبي يلحق المال، سواء أكان هذا المال مالا عاما أم مالا خاصا.

أما حجم الضرر وطبيعته ومدى شموله للمال بحيث يؤدي إلى انعدامه أو كونه جزئيا يعطل المال مع عدم إعدامه فلا ينظر إليه بقدر ما ينظر إلى تحققه بأية نسبة كانت.

[1] جلال محمد الزعبي، أسامة أحمد المناعسة، المرجع السابق، ص121.

القصد الجنائي.

لا بد لتحقق العقاب عن فعل الإتلاف المجرم بالنص من تحقق القصد الجنائي، هذا القصد الذي يقوم على عنصري العلم و الإرادة، العلم بطبيعة الفعل المراد القيام به وأثره ثم العلم بماهية المال محل الاعتداء، وأنه مملوك للغير، ثم تحقق عنصر القصد وهو إرادة هذا الفعل وإرادة النتيجة المرجوة منه، فإن اعتقد الفاعل أنه يتلف ماله لم تقع الجريمة، وإن اعتقد أنه لن يسبب بفعله هذا الإتلاف لم تقع الجريمة أيضا؛ هذا من حيث الأصل العام لجريمة الإتلاف.

ثانيا: الإتلاف والتجارة الإلكترونية

الإتلاف الإلكتروني أو المعلوماتي يختلف جوهريا عن الإتلاف التقليدي كجريمة، في فعل الإتلاف وطبيعته وماهيته من جهة، وفي طبيعة المال موضوع فعل الإتلاف من جهة أخرى؛ فهو نوع جديد من جرائم الإتلاف أظهرته الاستخدامات المتعددة واسعة النطاق لنظم المعلومات وتقنيات الاتصال المعلوماتي، في شتى مناحي الحياة العامة والخاصة، بالإضافة إلى التطور الفلسفي الذي أصاب مفهوم المال ومحددات ذلك ما يلي:

– السلوك الإجرامي في الإتلاف التقني هو السلوك الإلكتروني بالضرورة، فهو ليس سلوكا تقليديا، مواده الانتقال في عالم المحسوسات، واعتماده على الحركة والقوة لتحقيق النتيجة، بل السلوك هنا سلوك معنوي، يعتمد على تقنيات الحاسب الآلي، ونظم المعلومات وتقنيات الاتصال المعلوماتي، بعيدا كل البعد عن محاور الانتقال والحركة واستخدام عناصر القوة ونحو ذلك، فالسلوك هادئ وبسيط وسريع ،لا يكلف الفاعل أدنى جهدا أو وقت يحقق به الفاعل ذات النتائج إن لم تكن أعظم أثرا، ففي الوقت الذي كان يحقق فيه فعل الكسر تلفا للمال المادي، أصبح تحرير برنامج فاسد وإقحامه في نطاق حاسب آلي أو منظومة اتصال معلوماتي أقدر على تحقيق تلف عظيم في مال معلوماتي ذي قيمة لصاحبه.[1]

– بيئة إلكترونية بدل بيئة واقعية، فلا يعقل أن يظهر السلوك المعنوي إلا في بيئة معنوية، تتفق وخصائصه وميزاته. هذه البيئة الإلكترونية قوامها نظام حاسب آلي يعتمد على مكوناته، ذات الصفة

[1] الزعبي، المرجع السابق، ص122.

والطبيعة المعنوية لا المادية، لا يمكن لمسها، غير أنها موجودة وذات قيمة،ونظام معلوماتي قوامه حواسيب آلية وشبكات اتصال تشكل بمجملها بيئة إلكترونية معنوية، فيها أموال ذات خصائص معنوية هي محل الفعل بالإتلاف.

وعليه فإن طبيعة المال محل فعل الإتلاف وطبيعة السلوك المحقق لهذا الإتلاف كلاهما يعتمد على الآخر، وينبثق منه، فلا يتصور أحدهما دون الآخر، إذ لا إتلاف معنوي الكترونيا بلا مال الإلكتروني معنوي، ولا إمكانية لتصور إتلاف إلكتروني لا يكون محله مال الإلكتروني معنوي، وهو أمر لا يتوافر إلا في بيئة إلكترونية قوامها تقنية نظم المعلومات.[1]

– نتائج معنوية بدل نتائج مادية، فلم يعد بالإمكان مشاهدة آثار مادية لفعل الإتلاف تلمس أو تدرك بالحواس الظاهرية، وإنما انتقلنا وضمن نظرية الإجرام المستحدث إلى نتائج معنوية، اكتسب صفتها تلك من الطبيعة المعنوية للمال المعلوماتي محل فعل الإتلاف بصورته المستحدثة، فالبيانات والبرامج والمعلومات ووسائل الاتصالات ونظم المعلومات محل صالح لوقوع فعل الإتلاف عليها، وربما تكون الآثار السلبية للفعل أعظم أثرا من تلك الأفعال التي عرفتها البشرية في ظل البيئة المادية التقليدية،فالأضرار اللاحقة بتلك المكونات المعنوية هي الأخرى معنوية، ومن ذات الطبيعة، فإن تحقق الضرر المادي كنا أمام جريمة تقليدية لا مستحدثة.[2]

يتحقق الركن المادي في جريمة الإتلاف بإحدى صورتين:

الإتلاف المباشر: وصورته أن يتوسل الفاعل بصورة مشروعة أم بصورة غير مشروعة، وبأية طريقة كانت، للوصول إلى جهاز الحاسب الآلي ذاته، أو بإحدى مدخلات أو النهايات الطرفية لنظام معلوماتي ما، بصورة مباشرة بوصوله إلى لوحة المفاتيح مثلا، أو بوصوله إلى أحد منافد الدخول وبوابات العبور للنظام، ثم هو يقدم على سلوك تقني إلكتروني مباشر ويحقق به الإتلاف المقصود.

مثال ذلك من يدخل شركة ما، أما بصورة مشروعة، كونه أحد موظفيها، أو أن يدخل بصورة غير مشروعة، سواء أكان شخصا غريبا عنها، لا يسمح له بالدخول دون إذن معين، أو هو أحد موظفي

[1] المرجع نفسه ص123.

[2] المرجع نفسه، ص 123.

الشركة أو أحد العاملين فيها، إلا أنه لا يسمح له بدخول قسم معين فيها، إلا بإذن معين أيضا، فإذا كان ذلك الدخول إلى الشركة غير مشروع قام الفاعل بالوصول إلى أحد حواسيب نظم المعلومات، أو إحدى نهاياته الطرفية، ويعمد إلى إدخال رمز أو أمر معين، أو برنامج معين، ويسبب به إتلاف المعلومات أو البيانات المخزنة على النظام، وبصورة كلية أو جزئية، أو التعدي على نظم الاتصالات المعلوماتية بصورة أخرى.

الإتلاف غير المباشر: وصورته الوصول إلى نظام الحاسب الآلي أو نظم المعلومات عبر نافذة غير مباشرة، فالفاعل سواء أكان ذا علاقة بالنظام المعلوماتي محل الجريمة، أم كان غريبا عنه، فإنه لا يصل إلى لوحة المفاتيح الخاصة بالنظام بصورة مباشرة، كما هو الفرض السابق ولكنه يستخدم إحدى النهايات الطرفية للنظام، فيستغل وجود اتصال به لأية غاية، أو يستعين بأحد نظم و برامج الاختراق المعلوماتي، فيقتحم حواجز الحماية الخاصة بشبكات الاتصال المرتبطة بها، فيدخل إلى النظام ثم يتوصل بطريقة فنية تقنية إلى إتلاف المعلومات أو البيانات، أو تعطيل سبل الاتصالات.

المحل في جرائم الإتلاف التقني: بداية لا بد أن نشير إلى أن محل الإتلاف هنا المال المعلوماتي والذي تم بحثه بشكل مفصل سابقا، والذي رأينا أنه مال مقوم بمفهوم القانون قابل لحمايته صالح لوقوع فعل الإتلاف عليه.

المال المعلوماتي يأتي بإحدى صورتين كل منهما تصلح أن تكون محلا لفعل الإتلاف وهي:

الصورة الأولى: المال المعلوماتي المخزن على دعائم أو أقراص أو أي وسيلة لحفظ ومعالجة البيانات والمعلومات إلكترونيا، ويكون هذا المال المعلوماتي بهذه الصورة محلا صالحا لجريمة الإتلاف المتمثل بتدمير الدعامة المخزن عليها، تلك البيانات أو المعلومات كليا أو جزئيا، كما يتمثل فعل الإتلاف أيضا بتعطيل الدعامة ومنع الوصول إلى المعلومات والبيانات المخزنة عليها.

وتجدر الإشارة إلى أن المال المعلوماتي بهذه الصورة لا يمكن أن يكون محلا لفعل الإتلاف إلا بصورته المباشرة، ذلك أن وجود الدعامات وما عليها من بيانات يبقى بعيدا عن نظم الاتصال المعلوماتي أحد أهم وسائل الإتلاف غير المباشر.

الصورة الثانية: المال المعلوماتي الموجود على نظام معلومات ما، سواء كان موجودا ضمن أدوات تخزين حاسب آلي أو عدد محصور منه، أو كان موجودا عبر الانترنت؛ فإذا كانت الدعامات الإلكترونية صالحة لحفظ وتخزين المعلومات والبيانات، فليس ثمة صعوبة في أن تكون هذه المعلومات والبيانات موجودة خارج دعائمها، وأن تكون على نظم المعلومات وتقنية هذه النظم وجودا معنويا ذا أثر، وبهذه الحالة يكون المال المعلوماتي المجسد بها عرضة لفعل الإتلاف الإلكتروني بكل صوره، فقد يتم الإتلاف بصورة مباشرة أو غير مباشرة عبر الولوج غير المشروع إلى نظم المعلومات وإتلافها كليا أو جزئيا.[1]

يتحقق فعل الإتلاف غير المباشر بتحقق الاختراق أو الولوج غير المشروع إلى نظام معلوماتي ما، ثم تحقيق أهداف المخترق بالإتلاف، كليا كان أو جزئيا، ووسيلته في تحقيق الإتلاف فتكون من خلال استخدام الفيروسات المختلفة والتي لا يمكن حصرها، فمن فترة إلى أخرى تطالعنا الأحداث بظهور فيروس جديد يهدد عالم المعلوماتية.

أما الضرر في جرائم الإتلاف، فإن فعل الإتلاف يؤثر على نظم المعلومات والمعطيات بطرق مختلفة منها ما يلي:

- التأثير على المعطيات والمعلومات من خلال تدميرها كليا أو جزئيا، حجبها ومنع صاحبها من الوصول إليها، تحريفها بحيث تظهر بصورة غير حقيقية.
- التأثير على نظم المعلومات وذلك بمنع تشغيلها واستفادة صاحبها منها، تبطئتها، وتدميرها.

وبشكل عام فإن حجم الضرر وطبيعته لا يمكن حصرهما، ولكن يمكن إجمالهما فيما يلي:

- تباطؤ أداء جهاز الحاسب الآلي وجهاز الاتصالات.
- حدوث أخطاء عند تشغيل البرامج.
- زيادة حجم التخزين دون مبرر.
- سماع نغمات موسيقية غير مألوفة.
- حدوث خلل في أداء لوحة المفاتيح.
- إتلاف ملفات البيانات والمعلومات.

[1] الزعبي، المرجع السابق، ص 125.

– عدم القدرة على الوصول إلى ملفات التخزين.
– زيادة زمن قراءة القرص.

ومظاهر أخرى منها ما ينصرف إلى تخريب نظم الاتصالات ونظم المعلومات، ومنها ما ينصرف إلى تقليل قيمتها وفوائدها ومزاياها التشغيلية والتطبيقية، ومنها ما ينصرف إلى تعطيل نظم المعلومات وآليات عمل الشبكات كليا أو جزئيا سواء أتم ذلك بصورة دائمة أم مؤقتة.

أما الركن المعنوي في جريمة الإتلاف، فإن الإتلاف جريمة مقصودة سواء بصورتها المادية التقليدية أو بصورتها المعنوية المستحدثة التي يطلق عليها الإتلاف المعلوماتي، يقوم القصد على عنصري العلم والإرادة، العلم بالفعل ونتائجه ثم إرادة هذا الفعل وإرادة نتائجه، بغض النظر عن طبيعة السلوك وماهيته، أو حجم وطبيعة الضرر الناشئ عنه.[1]

المطلب الثاني: الحماية الجزائية للمستهلك الإلكتروني من الجرائم المستحدثة

يعالج هذا المطلب من خلال التطرق إلى جملة من المواضيع وهي حماية المستهلك الإلكتروني من الإعلانات الكاذبة أو الخادعة (الفرع الأول)، الحماية الجزائية لبطاقات الائتمان أو الدفع الإلكتروني (الفرع الثاني)، وحماية التوقيع الإلكتروني للمستهلك (الفرع الثالث).

الفرع الأول: حماية المستهلك من الإعلانات التجارية الإلكترونية الكاذبة أو الخادعة.

تلعب الإعلانات دورا مهما من الناحية التجارية، فعن طريقها يتمكن المستهلك من التعرف على السلعة أو الخدمة، ومواصفاتها، وسعرها، وكيفية الحصول عليها؛ غير أن الإعلانات – وخاصة في الوقت الراهن – قد لا تكون دائما صادقة ودقيقة، في وصف السلعة أو الخدمة، مما قد يوقع المستهلك في الغلط، ويبادر إلى التعاقد بناء على هذا الغلط الذي وقع فيه، وهذا الأمر يدعو إلى ضرورة حمايته قانونا، خاصة عن طريق القواعد الجزائية، وتزيد هذه الضرورة عندما يكون الإعلان عن طريق الوسائل الحديثة وخاصة الوسائل الإلكترونية، لما تتميز به من سرعة وإبهار وانتشار واسع،

[1] الملط، المرجع السابق، ص548.

كما أن الإعلان أو الإشهار التجاري يعتبر مظهرا من مظاهر المنافسة المشروعة، فإن كان مضللا أو خادعا كان له أثره السلبي على منظومة المنافسة الحرة كلها، وحق المستهلك في تلقي معلومات صحيحة عن السلع والخدمات.[1]

بناء على ما تقدم، يعالج هذا الفرع من خلال التطرق إلى التنظيم القانوني للإعلانات التجارية الإلكترونية، ثم الحماية الجزائية للمستهلك من الإعلانات الإلكترونية الخادعة أو الكاذبة.

أولا: التنظيم القانوني للإعلانات التجارية الإلكترونية.

جاء تعريف الإعلان[2] التجاري في المادة الثالثة من القانون الفرنسي رقم 1150/79 الصادر في 1979/12/29 بشأن الحماية من اللافتات الإعلانية المعلقة على الجدران كما يلي: "يعتبر إعلانا كل نقش يهدف إلى إعلان الجمهور وجذب انتباهه، سواء كان نقشا نموذجيا أو صورة ."[3]

أما التوجيه الأوربي الصادر سنة 1984 بقصد التقريب بين تشريعات الدول الأوربية المشتركة فقد عرف الإعلان بأنه: "أي شكل من أشكال الاتصالات تتم في مجال الأنشطة التجارية أو الصناعية أو الحرفية أو المهنية، وتهدف إلى تشجيع الإقبال على السلع والخدمات بما في ذلك العقارات والحقوق والالتزامات المرتبطة بها".[4]

عرف المشرع الجزائري في المادة الثانية من المرسوم التنفيذي رقم 90-39 المؤرخ في 30 يناير 1990 المتعلق برقابة الجودة وقمع الغش،[5] الإعلان مستخدما لفظ الإشهار بأنه: "جميع

---

[1] ياسين آيت أحمد، الضوابط القانونية لحماية المستهلك في مجال الإشهار، مجلة العلوم القانونية، العدد الثاني، مطبعة الأمنية، الرباط، المملكة المغربية 2014، ص184.

[2] يستخدم المشرع الجزائري مصطلح إشهار عوض إعلان، غير أنه استخدم مصطلح إعلان في م04، واستخدم المصطلحين معا في م52 من المرسوم التنفيذي 13-378 المؤرخ في 2013/11/09، والمحدد للشروط والكيفيات المتعلقة بإعلام المستهلك، ج ر 58.

[3] خالد ممدوح إبراهيم، حماية المستهلك في العقد الالكتروني، دار الفكر الجامعي، الإسكندرية 2008، ص 134.

[4] المرجع السابق، ص135.

[5] ج ر عدد 50 لسنة 1990.

الاقتراحات والدعايات أو البيانات والعروض أو الإعلانات أو خدمة بواسطة إسناد بصرية أو سمعية بصرية".

كما عرفه من خلال المرسومين التنفيذيين 101/91، و103/91، وعرفه مرة أخرى بموجب م2 من القانون 02/04 المؤرخ في 23 جوان 2004 المحدد للقواعد المطبقة على الممارسات التجارية بأنه: "كل إعلان يهدف بصفة مباشرة أو غير مباشرة إلى ترويج بيع السلع أو الخدمات مهما كان المكان، أو وسائل الاتصال المستعملة".

أما المشرع التونسي فعرفه في الفصل 35 من قانون عدد 40 لسنة 1998 المتعلق بطرق البيع والإشهار التجاري بأنه: "كل عملية اتصال تهدف بصورة مباشرة أو غير مباشرة إلى تنمية بيع منتجات أو إسداء خدمات مهما كان المكان أو وسائل الاتصال المعتمدة".[1]

ويعرفه بعض الفقه بأنه: "مجموعة من الجهود التي تهدف إلى توجيه انتباه أفراد المجتمع إلى سلعة أو خدمة محددة، لحثهم على شرائها أو طلبها، أو هو عبارة عن أنواع الأنشطة المختلفة التي يتم من خلالها نشر أو إذاعة الرسائل الإعلانية المرئية أو المسموعة على أفراد المجتمع، بهدف حثهم على شراء السلعة أو طلب الخدمة المعلن عنها".[2]

وللإعلان أهمية بالغة في التعريف بالخدمات والمنتجات، ووجودها ومدى وفرتها، وقدرتها على الوفاء بحاجات المستهلك، وأصبحت له فوائد كبيرة، كما أنه يحيط بالإنسان من كل جانب،[3] عن يمينه وعن شماله، ومن خلفه، ومن فوق رأسه، فلا مفر منه، إذ غدا واقعا مفروضا.[4] ومنذ صدور أولى الجرائد المطبوعة بواسطة الروتاتيف، من حوالي قرن ونصف أو يزيد من الزمن، وعالم الاتصال يضاف إليه كل ربع قرن تقريبا تقنية جديدة، إلى أن وصلنا إلى ما

[1] ياسين آيت أحمد، المرجع السابق، ص185.

[2] خلوي نصيرة، الحماية القانونية للمستهلك عبر الانترنت، مذكرة لنيل شهادة الماجستير في القانون، فرع المسؤولية المهنية، جامعة مولود معمري تيزي وزو 2013، ص11.

[3] أ.د بودالي محمد، الحماية القانونية للمستهلك عن الإشهار الكاذب أو الخادع، مجلة العلوم القانونية والإدارية، العدد 6، سيدي بلعباس 2009، ص11.

[4] المرجع نفسه، ص12.

يسمى اليوم ثورة المعلومات التي أفرزت مجتمعا جديدا هو مجتمع الإعلام والمعلومات أبرزُ سماته الملتيميديا المباشرة وهي نتيجة تمازج بين الإعلام الآلي، والاتصالات السلكية واللاسلكية ووسائل الاتصال.[1]

ولا يختلف الإعلان الإلكتروني عن الإعلان التقليدي إلا من حيث الوسيلة المستعملة، إذ يعتمد الإعلان الإلكتروني على وسائل تقنية حديثة كالانترنت والهاتف المحمول والفاكس والتلفزة الرقمية والراديو الرقمي والأقراص المضغوطة على اختلاف أنواعها وغيرها، وهذه الوسائل تضفي خصوصية على الإعلان.

ويتفق الفقه مع أحكام القضاء المتواترة على اعتبار الدعائم الإلكترونية للإعلانات كالدعائم التقليدية، وتطبيق ذلك في الحكم الصادر عن محكمة استئناف "ران" الفرنسية الصادر في 31 مارس 2000،[2] والحكم الصادر عن محكمة استئناف باريس في 03 مايو 2001 المتعلق بالإعلانات غير المشروعة التي تمثل اعتداء على علامة تجارية مملوكة للغير، والحكم الصادر عن محكمة "ماكون" الابتدائية الصادر في 24 أبريل 2001 الخاص بالدعاية الكاذبة على شبكة الانترنت.[3]

---

[1] فندوشي ربيعة، الإعلان عبر الانترنت، مذكرة ماجستير في علوم الإعلام والاتصال، جامعة الجزائر 2005/2004، ص102 و103.

2 تتلخص وقائع القضية في أن بنك crédit mutuel أسس موقعا عبر شبكة الانترنت يعلن فيه عن مزايا بطاقة الائتمان الخاصة به، وأو ضح من خلال الإعلان شروط الحصول عليها وطريقة عملها. طعن أحد الأشخاص في هذا الإعلان على أساس أنه خادع، لأنه لم يحدد باقي شروط العقد الخاص بالقرض، وبالأخص مدة القرض والفائدة المستحقة للبنك، ورد البنك بأن الانترنت لا تعد دعامة إعلانية بالمعنى المتعارف عليه، ومن ثم لا تعد الإعلانات التي تبث عبرها إعلانات تجارية بالمعنى الدقيق للكلمة، وبالتالي لا تخضع للنصوص التي تحكم الإعلانات الكاذبة أو الخادعة. غير أن المحكمة دحضت هذه الحجج كالآتي: إن الانترنت تسمح كغيرها من الدعامات الإعلانية الأخرى بالاتصال بالجمهور من خلال نص مكتوب أو صورة أو صوت، وتتيح لهم الإطلاع على أسعار وطبيعة السلع والخدمات التي تعرضها الشركات المختلفة، وواقعة أن صفحة الانترنت لا يمكن الإطلاع عليها إلا من خلال اشتراك معين في بعض المواقع أو على الأقل باختيار المستهلك لها ودخوله إليها، لا تغير من الخاصية الإعلانية للانترنت؛ فدخول المستهلك إلى الموقع يشبه شراءه الجريدة التي تحتوي على الإعلانات؛ فالخاصية المميزة للدعامة الإعلانية تكمن في أنها تسمح ببث الإعلانات عليها أيا كان شكل هذه الدعامة، وتقوم بحث المستهلك على شراء السلع وطلب الخدمات، وهذه الخاصية لا ريب أنها تتوافر في الانترنت. يراجع: د شريف محمد غنام، التنظيم القانوني للإعلانات التجارية عبر شبكة الانترنت، دار الجامعة الجديدة، الإسكندرية مصر 2011،ص ص5-6.

[3] المرجع نفسه، ص06.

ويرى البعض أن القضاء الألماني كان له السبق في اعتبار الدعامات الالكترونية وخاصة الانترنت، كالدعامات التقليدية بالنسبة للإعلانات التجارية.[1]

الواقع إذن أن الإعلان التجاري "التقليدي والإلكتروني" قد يستخدم في خداع المستهلكين، ولهذا الأمر عواقب وخيمة عليهم وعلى الاقتصاد عامة، كما يقوض من ركائز المنافسة الشريفة بين الشركات، لذا اهتمت التشريعات المقارنة بتجريم الإعلان الكاذب أو الخادع؛[2] ففيما يخص التشريعات الوطنية فقد اهتمت الدول المختلفة بهذا الموضوع، وتنقسم القواعد التي يمكن أن تُستمد من القوانين الوطنية إلى ثلاثة أنواع، أولها تلك القوانين التي لا تنظم الإعلانات التجارية مباشرة، ولكنها تتضمن بعض النصوص المتعلقة ببعض نشاطاتها، ومن أمثلة ذلك قوانين الملكية الفكرية، وحماية المنافسة، وحماية المستهلك، وبعض النصوص العامة في قانون العقوبات...وثانيها تتعلق بالقواعد التي تنطبق على الإعلانات التجارية "التقليدية" ولكنها قابلة للتطبيق على الدعائم الإلكترونية، ومن أمثلة ذلك القانون الفرنسي الصادر في 1979/12/29 الخاص بالإعلانات التجارية والإشارات المرئية سالف الذكر، والقانون الخاص بالاتصالات السمعية البصرية الصادر في 1986/09/30، والقوانين الجزائرية ذات الصلة بالإشهار، والقوانين المصرية ذات الصلة؛ أما النوع الثالث والأخير فيتعلق بالقواعد التي تنظم الإعلانات التجارية التي تتم عبر الانترنت والوسائل الإلكترونية الأخرى، أو المسائل المرتبطة بها ارتباطا مباشرا، ومن أمثلة هذا النوع في فرنسا القانون الصادر في 2000/03/23 المعدل لقانون 1986/09/30 المتعلق بالاتصالات السمعية البصرية، والقانون الصادر في 2004/06/21 المتعلق بالثقة في الاقتصاد الرقمي والقانون الصادر في 2005/02/24 معدلا لقانون "Evin" الخاص بتنظيم الدعاية التجارية عن الكحوليات عبر شبكة الانترنت.[3]

لقد حاولت الدول الأوربية أيضا تنظيم مسألة الإعلانات التجارية الإلكترونية، بإصدار توجيهات منسقة لبعض الأمور القانونية، فبالإضافة إلى التوجيهات المنظمة لموضوعات لا تمس مباشرة الإعلانات التجارية، ولكنها تقبل التطبيق عليها بطريقة أو بأخرى، عرفت أوربا توجيهات عدة تتعلق

[1] المرجع نفسه، ص06.

[2] بودالي محمد، المرجع السابق، ص16.

[3] شريف محمد غنام، المرجع السابق، ص11.

بالإعلانات الإلكترونية، من مثل التوجيه الصادر في 2000/06/08 بخصوص خدمة مجتمع المعلومات، وبصفة خاصة في التجارة الإلكترونية، والتسويق عبر الانترنت، وهو التوجيه المعروف باسم توجيه التجارة الإلكترونية، والتوجيه الصادر في 2002/07/12 المتعلق بحماية البيانات الشخصية وحماية الخصوصية في مجال الاتصالات الإلكترونية، والتوجيه الصادر في 2004/04/29 المتعلق بحماية حقوق الملكية الفكرية.[1]

بالإضافة إلى هذه الجهود هناك ما يعرف بالتنظيم الذاتي للإعلانات التجارية الإلكترونية، والهدف منه تحقيق ضبط ذاتي للإعلانات التجارية، من ذلك أعمال النقابة الوطنية للاتصال المباشر في فرنسا، والتي تتضمن توصيات وتوجيهات للشركات المنضمة إليها، والقائمةُ التي أعدتها النقابة الفرنسية لمشروعات البيع بالمراسلة والبيع عن بعد، وهي تجمع كل أسماء المستهلكين غير الراغبين في تلقي إعلانات تجارية في بريدهم الإلكتروني، وتقنينُ حسن السلوك الذي أعدته CNCI (Conseil Scientifique Médecine) عن Spam [2].

ثانيا: الحماية الجزائية للمستهلك من الإعلانات التجارية الإلكترونية الكاذبة أو الخادعة.

لا توجد نصوص خاصة في القانون الجزائري تجرم الإعلان الكاذب أو الخادع[3] سواء أكان إعلانا تقليديا أم إلكترونيا، الأمر ذاته عاشته فرنسا قبل سنة 1963، مما جعل القضاء الفرنسي – في غياب النصوص الخاصة – يلجأ إلى تطبيق القواعد العامة المتعلقة بجريمة النصب، ونصوص أخرى تعاقب على الغش والتدليس ونصوص أخرى متعلقة بالرسوم والنماذج الصناعية والبيانات والعلامات والأسماء التجارية.[4]

حري بنا معرفة ما المقصود بالإعلان الكاذب والإعلان الخادع أو المضلل.

---

[1] المرجع نفسه، ص12.

[2] Communication électronique non sollicitée en premier lieu via le courier électronique

يراجع: شريف محمد غنام، المرجع السابق، ص15.

[3] عرفت الجزائر في تاريخها ثلاثة مشاريع لقانون الإشهار، سنوات 1988، 1992، و1999، عكس كل واحد منها التوجه الاقتصادي والسياسي في كل فترة، وقد أشارت بعض المواد في هذه المشاريع إلى الإعلان الكاذب أو الخادع. يراجع:

بوراس محمد، الإشهار عن المنتجات والخدمات، أطروحة دكتوراه في القانون الخاص، جامعة أبي بكر بلقايد، تلمسان 2012/2011، ص425.

[4] بودالي محمد، المرجع السابق، ص19.

يرى البعض – بحق – أن الخداع أشمل وأوسع من حيث المدلول من الكذب، فالكذب أحد وسائل الخداع، والإعلان قد يكون مضللا، لأنه يتضمن أكاذيب، ويكون أيضا مضللا بسبب تغاضيه عن الحقيقة أو كتمانه لها أو عرضها بطريقة منقوصة، مما يجعل المستهلك يقع في لبس.[1] وعليه، يمكن القول أن تعبير الإعلان الخادع يشمل الإعلان الكاذب والمضلل، وقد استخدم المشرع اللبناني مصطلح الإعلان الخادع، بدل الإعلان التضليلي الذي استخدمه مشرعنا في م28 من القانون 02/04 سالف الذكر، ولكن المشرع الجزائري استخدم لفظ الخداع في م68، م69 من قانون حماية المستهلك رقم: 03/09 بصدد تطرقه لجريمة الخداع.[2]

ويرى الفقه أن الإعلان الكاذب هو ذلك الإعلان الذي به تغيير وتزييف للحقيقة وإظهار الشيء على غير حقيقته؛ ولا يطلب القانون من المعلن قول الحقيقة كاملة، بل يكفي أن يصدق في ذكره للمواصفات والمعلومات المعلن عنها، فالمستهلك الحالي لا ينتظر حقيقة مطلقة ولكنه أيضا لا يتوقع معلومات ضارة مخالفة للحقيقة، أما الإعلان الخادع أو المضلل فهو الذي لا يتضمن معلومات كاذبة ولكنه يصاغ في عبارات أو صور من شأنها أن تترك انطباعا غير حقيقي لدى المستهلك عن الشيء المعلن عنه يدفعه نحو التعاقد نتيجة انخداعه بالإعلان، ويكون الإعلان خادعا كذلك عندما يتغافل المعلن عن ذكر البيانات الجوهرية للمنتج،[3] وهذا ما حذا بالمشرع في القوانين المقارنة إلى إرساء مبدإ: واجب إعلام المستهلك عن المنتج أو الخدمة، ويقتضي ذلك أن يكون الإعلان الإلكتروني واضحا، بمعنى أن يتضمن البيانات الكافية عن السلعة أو الخدمة، والتي من شأنها بلورة رؤية واضحة وتفكير واع متبصر، يعمل على تكوين إرادة واعية مستنيرة لدى المستهلك وهو بصدد الإقبال على التعاقد، وهذا ما أشار إليه المشرع الفرنسي، ففي القانون الفرنسي الصادر سنة 1986 المتعلق بالوسائل السمعية البصرية إلزام واضح للمعلنين بأن تكون إعلاناتهم واضحة وخالية من اللبس والغموض.[4]

[1] ياسين آيت أحمد، المرجع السابق، ص192.

[2] بوراس محمد، المرجع السابق، ص271.

[3] خليفي مريم، المرجع السابق، ص249.

[4] خالد ممدوح إبراهيم، المرجع السابق، ص147.

يتخذ الإعلان الإلكتروني الخادع أساليب متعددة تهدف كلها إلى حجب الحقيقة عن جمهور المستهلكين، وقد يستعمل المعلنون ألفاظا مضللة تتعلق بالأسعار، كالإعلان عن تخفيضات دون تحديد المدة ولا السلع المعنية بالتخفيض، أو تتعلق بنوعية الخدمة أو جودة السلع، وما يترتب عن هذه الألفاظ الجذابة أو الرنانة من تأثير في الجمهور إذا تجاوزت الحد المعقول والمألوف من طرف المستهلكين.[1]

ويشكل المضمون الزائف كله أو بعضه للرسالة الإعلانية الركن المادي في جريمة الإعلان الكاذب، أما الركن المعنوي للجريمة فانقسم الفقه الفرنسي بشأنه بين قائل بضرورة توفر القصد الجنائي المتمثل في سوء النية، وقائل بعدم ضرورة توافر سوء النية، وقائل بضرورة التفرقة في شدة الجريمة على ضوء سوء النية أو حسنها بحيث يعتبر المعلن سيء النية مرتكبا لجنحة، والمعلن حسن النية مرتكبا لمخالفة، وقائل بأن سوء النية في الإعلان الكاذب مفترض، بحيث يصير عبء الإثبات على المعلن الذي يتوجب عليه إثبات حسن نيته لتجنب المتابعة.[2] ومعيار تقدير الكذب موضوعي ينظر فيه إلى المستهلك متوسط الذكاء والحذر واليقظة.

أما الركن المادي في جريمة الإشهار المضلل أو الخادع "publicité trompeuse" فيتمثل في كل ما من شأنه أن يخلق لبسا من شأنه أن يؤدي إلى خداع المستهلك،[3] أي إيقاعه في الخطأ، ولا يشترط أن يكون الإعلان مضللا في ذاته،[4] ويتحدد التضليل وفق المعيار الموضوعي، بمعنى أن الإعلان من شأنه خداع أو تضليل المستهلك العادي، مع ترك مسألة تقدير إن كان الإعلان مضللا أم لا للقضاء.[5]

---

[1] ياسين آيت أحمد، المرجع السابق، ص192.

[2] بوراس محمد، المرجع السابق، ص ص272-274.

[3] خالد ممدوح إبراهيم، أمن الجريمة الإلكترونية، الدار الجامعية، الإسكندرية مصر 2008، ص126.

Le tribunal correctionnel de Lyon avait décidé dans un jugement rendu le 3 février 2005, que constituait un délit de publicité trompeuse le fait pour un site d' e-commerce d'annoncer des délais de livraison très rapides et de ne pas les respecter. La cour d'appel de Lyon a confirmé cette décision dans un arrêt rendu le 7 mars 2007(Condamnation du PDG du site "Père-Noël.fr" pour publicité mensongère). Voir le site : légalis.net.

[4] خالد ممدوح إبراهيم، حماية المستهلك في العقد...المرجع السابق، ص151.

[5] المرجع نفسه، ص152.

Par un arrêt du 29 janvier 2013, la chambre commerciale de la Cour de cassation remet en cause la décision d'appel sur la publicité trompeuse, qui a, selon elle, été retenue pour des motifs impropres à caractériser cette infraction, en application des critères énumérés par l'article L. 121-1 du code de la consommation.
Dans cette affaire, à chaque fois qu'un internaute effectuait une recherche sur Google avec le terme Cobrason, il accédait automatiquement à une page de résultat diffusant une annonce publicitaire renvoyant vers le site d'une société concurrente, également spécialisée dans la vente de matériel hi-fi. La cour d'appel avait jugé que

نتساءل الآن: ما العمل في الجزائر، في ظل غياب نصوص خاصة تعاقب على جريمة الإعلانات الإلكترونية الخادعة أو الكاذبة؟

هناك عدد من الحلول، أولها سن نصوص خاصة تعالج هذه المشكلة.

في انتظار ذلك، يجوز للقضاء الجزائري أن يقتدي بنظيره الفرنسي قبل سنة 1963، ويلجأ إلى نصوص عقابية أخرى، منها القواعد العامة المتعلقة بجريمة النصب، بموجب م372 ق ع، وجريمة الخداع بموجب م429 ق ع، ونصوص أخرى، إلا أن هذه النصوص لا توفر الحماية المطلقة، فجريمة النصب تتطلب شروطا دقيقة لقيامها منها عدم الاعتداد بمجرد الكذب غير المقترن بأعمال مادية أو وقائع خارجية أو بنوع من الحبك المسرحي، كما أنها تتطلب أن يكون الهدف من استخدام الطرق الاحتيالية الوصول إلى تحقيق أمر مما هو منصوص عليه على سبيل الحصر في النص العقابي، وهو ما لا يتوافر دوما في الإعلانات الكاذبة أو الخادعة.[1] كما أن جريمة الخداع لا توفر حماية كافية لما تتطلبه لأجل قيامها، فهي تستلزم وجود عقد تجاه شخص معين متعاقد، الأمر الذي لا تقوم معه الجريمة إذا لم يتبع الإعلان تعاقد، كما أنها لا تنطبق إذا تعلق موضوع الجريمة بعقارات أو خدمات.[2]

كما يمكن إعمال نصوص قانون حق المؤلف والحقوق المجاورة في حالات معينة لحماية المستهلك من الإشهار الكاذب أو المضلل، غير أنه من النادر أن يكون الإشهار تقليدا وفقط لإبداع فكري.[3]

في القانون المصري وبعد صدور قانون حماية المستهلك رقم 67 لسنة 2006 أوجد المشرع حماية للمستهلك من الوقوع في الغلط، عن طريق إلزام المعلن والمورد بإعلام المستهلك بالمعلومات

---

l'apparition de ce lien commercial avait nécessairement généré une confusion dans l'esprit de la clientèle potentielle et provoqué, de ce seul fait, un détournement déloyal de clientèle ainsi qu'une utilisation parasitaire de l'investissement effectué par Cobrason au travers de son site et de l'organisation de ses campagnes publicitaires. En proposant le mot clé Cobrason, la société Google Inc « a également contribué techniquement à la confusion générée dans l'esprit du public intéressé », avait estimé la cour de Paris. Voir le site : légalis.net.

[1] بودالي محمد، المرجع السابق، ص23.

[2] المرجع نفسه، ص26.

[3] بوراس محمد، المرجع نفسه، ص410.

الصحيحة عن طبيعة السلعة وخصائصها بما يحمي المستهلك من تكوين اعتقاد غير صحيح، تحت طائلة العقوبة المقررة في م24 من القانون.[1]

الأمر ذاته بالنسبة للمشرع الجزائري بعد صدور المرسوم التنفيذي 13-378 المتعلق بإعلام المستهلك، سالف الذكر، الذي تطرق في م13/3 منه إلى تقنية الاتصال عن بعد، وعرفها بأنها كل وسيلة بدون الحضور الشخصي والمتزامن والمتدخل للمستهلك، يمكن استعمالها لإبرام العقد بين هذين الطرفين، كما تطرقت م4 من المرسوم ذاته إلى الإعلان كأحد وسائل إعلام المستهلك، كما أن م36 من المرسوم نفسه تطرقت إلى ضرورة ألا يوصف أو يقدم أي غذاء بطريقة خاطئة أو مضللة أو كاذبة، أو من المحتمل أن تثير انطباعا خاطئا بخصوص نوعه بطريقة تؤدي إلى تغليط المستهلك...كما أن م56 من المرسوم سالف الذكر نصت على منع كل معلومة أو إشهار كاذب من شأنهما إحداث لبس في ذهن المستهلك، الأمر نفسه نصت عليه م1/60، أما م2/60 فمنعت كل بيان يرمي إلى التمييز المفرط لمنتوج (منتَج) على حساب منتوج مماثل آخر (الإعلان المقارن). أما المادة 62 من فتطرقت إلى جزاء الإخلال بما جاء في هذا المرسوم، وأحالت ذلك إلى القواعد العامة ولا سيما أحكام القانون 09-03 المتعلق بحماية المستهلك وقمع الغش.

أما الإعلان المقارن فتسمح به بعض التشريعات وتحظره أخرى، وقد عرفه التوجيه الأوربي الصادر في 06 أكتوبر 1997 بأنه: "كل إعلان يؤدي صراحة أو ضمنا إلى التعرف على سلعة أو خدمات منافس آخر"، وقد عرفه المشرع المغربي في م22 من القانون 08-31 بأنه: "كل إشهار يقارن بين خصائص أو أسعار أو تعريفات السلع أو المنتوجات أو الخدمات، أو بالإشارة إلى عملية الصنع أو التجارة أو الخدمة الخاصة بالغير، أو تجسيدها وإما بالإشارة إلى العنوان التجاري وتسمية الشركة أو الاسم التجاري أو الشعار الخاص بالغير، أو تجسيد ذلك"، وللإشهار المقارن أهمية في إبراز إيجابيات وسلبيات الخدمة أو السلعة باتباع أسلوب المقارنة، ويضمن الشفافية والنزاهة والمنافسة الحرة، ويمكن المستهلكين من الحصول على إعلان صادق للسلع والخدمات، ويشترط أن تكون المقارنة صادقة وحقيقية، لا يشوبها تضليل من شأنه إيقاع المستهلك في الغلط، كما يجب أن تكون المقارنة نزيهة وموضوعية منصبة على العناصر الرئيسة والمفيدة للمستهلك، ويمكن التحقق منها، وتخص السلع

[1] خالد ممدوح إبراهيم، أمن الجريمة الإلكترونية، المرجع السابق، ص131.

والخدمات من الطبيعة نفسها، ولا ينبغي بأي حال من الأحوال اتخاذ الإعلان المقارن مطية للإضرار بالمنافسين والتشهير بمنتجاتهم،[1] كما ينبغي للإعلان المقارن أن يشير إلى المدة التي يحتفظ خلالها بالأسعار والتعريفات، ويعتبر كل إعلان مقارن لا يحترم الشروط المذكورة أعلاه إعلانا مضللا، لأنه يهدف إلى النيل من المنتجات المنافسة وتشويه سمعتها، من جهة، وخلق نوع من اللبس لدى أذهان المستهلكين نتيجة اختلاط الأمور عليهم من جهة ثانية.[2]

ولا يختلف الإعلان الإلكتروني المقارن عن الإعلان التقليدي المقارن سوى أنه يتم عبر وسيلة إلكترونية.

الإعلان المقارن جائز في القانون الفرنسي بشرط أن يكون موضوعيا لا يتناول سوى الخصائص الأساسية للسلعة أو الخدمة، وأن يكون أمينا صادقا ولا يؤدي إلى تضليل المستهلك، مع ضرورة أن يحصل المعلن عن موافقة المنافس الذي تضمنه إعلانه المقارن قبل عملية نشر الإعلان.[3]

---

[1] ياسين آيت أحمد، المرجع السابق، ص195.

أكدت محكمة الاستئناف التجارية بالدار البيضاء المغربية في قضية إشهار منتج "هلا" على القناة الثانية 2M، المملوك لشركة "صافيولا" ضد شركة "لوسيور" على ضرورة أن يكون الإعلان المقارن ضمن قواعد الشرف والمنافسة المشروعة، إذ جاء في حيثيات القرار: "حيث أن الإشهار الممنوع قانونا هو ذاك الذي يكون الهدف منه تحقير منتج والنيل منه، إن إجراء المقارنة بين منتَجين أو أكثر من أجل عرض خصائصها وعناصرها المميزة دون التشهير بالمنتَج المنافس تنتفي معه عناصر المنافسة غير المشروعة". المرجع نفسه، ص196.

[2] ياسين آيت أحمد، المرجع السابق، ص196.

جاء في قرار لمحكمة فرساي في 2010/03/18، 09/00672:

"La publicité comparative est autorisée si elle est loyale et véridique et n'est pas de nature à induire en erreur le consommateur et que la comparaison est déterminée et déterminable.
La publicité comparative ne doit pas être parcellaire et doit résulter d'une étude exhaustive et, qu'il appartenait à la société mise en cause de vé- rifier que les prix auxquels elle s'est référée dans sa publicité étaient représentatifs du prix de vente des produits sur le marché et qu'elle fondait sa comparaison sur des informations sincères et véridiques.
Il s'ensuit que la société mise en cause s'est livrée à une publicité trompeuse et comparative illicite caractérisant un acte de concurrence déloyale ". Affaire : S.A. EPSON France C/S.A. BOX OFFICE. voir le site :www.legifrance.gov.fr.

[3] خالد ممدوح إبراهيم، المرجع السابق، ص133.

الفرع الثاني: الحماية الجزائية لبطاقات الائتمان.

تعتبر بطاقات الائتمان أهم طرق الدفع بالنسبة للتجارة الإلكترونية،[1] وقد ساعد وجود هذه البطاقات وتطورها إلى درجة كبيرة في وجود وازدهار التجارة الإلكترونية، بل إن هذه البطاقات هي عصب التجارة الإلكترونية، ولأدل على ذلك ما أولته الوثائق الصادرة عن لجنة الأمم المتحدة للقانون التجاري الدولي من اهتمام بها، والتي أكدت على أهمية هذه البطاقات سواء في قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية الصادر عام 1996، أو دليل الأونسيترال النموذجي بشأن التجارة الإلكترونية الصادر عام 1996، أو قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية الصادر عام 2001، أو دليل اشتراع قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية الصادر عام 2001.[2]

غير أن هذه البطاقات ليست آمنة دوما، ويمكن اعتبارها سلاحا ذا حدين فإلى جانب مزاياها أو وظائفها المتعددة، ظهرت أمور سلبية، حيث ساعد ظهور هذه البطاقات وانتشارها على شيوع الجريمة بمختلف أشكالها، وانعكس بدوره على تطور أساليب ووسائل ارتكاب الجرائم وبروز أنواع من الجرائم غير المألوفة، تلك التي لم يفرض لها القانون قواعد عقابية، إذ أن الجريمة في هذا النطاق تتطور بصورة سريعة وذلك بما تقدمه الوسائل التكنولوجية من تسهيلات كبرى للأنشطة الإجرامية سواء المنظمة منها أو الفردية، والتي تبقى بعيدا عن العقاب، أما التشريعات والقوانين فهي بطيئة نسبيا وتتأخر عن مواكبة التغيرات التي تطرأ على وسائل التقدم العلمي المتجدد باستمرار، لذا بات من الضروري توفير حماية قانونية فعالة لهذه البطاقات، والبحث عن التكييف القانوني للصور المختلفة لجرائم بطاقات الائتمان، ناهيك عن تطوير تقنيات الحماية الفنية لها، وتعزيز التعاون مع المنظمات العالمية الرائدة للاستفادة من خبراتها في هذا المجال.[3]

---

[1] يستخدم الكثير من الكتاب مصطلح بطاقة ائتمان، وهم يقصدون جميع أنواع البطاقات: بطاقات وفاء، ائتمان أو حتى بطاقات السحب فقط، ويمكن إرجاع ذلك إلى التماثل الكبير بينها من حيث الشكل والمادة المستخدمة والوظيفة، إلا أن هناك فارقا بين بطاقات الوفاء وبطاقات للائتمان، وهو أن بطاقات الوفاء لا تمنح أصحابها ائتمانات مجانية على خلاف بطاقات الائتمان، فهي بطاقات وفاء فقط، وحتى بطاقات الوفاء ذات المديونية المؤجلة فهي لا تمنح الحامل إلا ائتمانا مجانيا قصير المدة لا يتعدى ستة أسابيع، لذلك تبقى بطاقة وفاء. يراجع: د. محمد نور الدين سيد عبد المجيد، المسؤولية الجنائية عن الاستعمال غير المشروع لبطاقات الوفاء والائتمان، دار النهضة، القاهرة 2008، ص13.

[2] أمير فرج يوسف، بطاقات الائتمان... مرجع سابق، ص212.

[3] أمير فرج يوسف، المرجع السابق، ص177-179.

ويرى البعض أن المشكلة الرئيسة في نظام التجارة الإلكترونية تتمثل في نظام الوفاء بالثمن نظير السلعة أو الخدمة، لما يكتنف ذلك من مخاطر جمة تتمثل في وضع تفاصيل البطاقة الائتمانية على شبكة الانترنت، لذلك فإن التجارة الالكترونية رغم تطورها المبهر، إلا أنها لم تبلغ حتى الآن الازدهار الذي كان متوقعا لها، بسبب تخوف المستهلكين من كشف بيانات البطاقة، خصوصا الرقم السري، مما يجعلها عرضة للاستغلال من قبل طائفة من المجرمين هم أشد خطورة من غيرهم.[1]

وفي ظل غياب نصوص خاصة بالنسبة لبعض الدول، يثور تساؤل مهم: هل النصوص التقليدية لقانون العقوبات كفيلة بتحقيق الحماية المطلوبة؟

لحماية بطاقات الائتمان قانونيا ينبغي أولا تحديد مفهوم الاستخدام غير المشروع لهذه البطاقات، حيث يجب تجريم كل استخدام غير مشروع، ولقد حاول البعض إعطاء تعريف للاستخدام غير المشروع لبطاقات الائتمان كالآتي: "يعتبر استخداما غير مشروع للبطاقة عندما يخل الحامل بشروط عقد إصدار البطاقة بما يؤدي إلى فسخ هذا العقد، أو قفل الحساب الذي تقوم البطاقة

---

[1] د. محمد نور الين سيد عبد المجيد، المسؤولية الجنائية عن تزوير بطاقات الائتمان، دار النهضة، القاهرة2012، ص66.

ذكرت شبكة MSNBC أن الحصول على أرقام البطاقات الائتمانية من شبكة الانترنت أمر في غاية البساطة، وعرضت قوائم تحتوي على أكثر من 2500 رقم بطاقة ائتمانية حصلت عليها من سبعة مواقع للتجارة الإلكترونية، عن طريق استخدام قواعد بيانات متوافرة تجاريا، يستطيع أي أحد الحصول عليها، واستخدامها في عملية شراء يدفع الثمن فيها أصحاب البطاقات الحقيقيون. وأكد وزير الداخلية المصري للمعلومات بأن جرائم الاستخدام غير المشروع للبطاقات تكلف مصر حوالي ثلاثة ملايين جنيه مصري سنويا. يراجع: عائشة بن قارة مصطفى، حجية الدليل الالكتروني في مجال الإثبات الجنائي، دار الجامعة الجديدة، الإسكندرية، مصر2010، هامش2، ص38.

تذكر الصحف الأمريكية أن ملايين الأمريكيين قد يجدون أنفسهم بين عشية وضحاها مدينين بآلاف الدولارات لمحلات قد لا يعرفون حتى أسماءها، بسبب من يسمون "لصوص الهوية"، الذين يتمكنون من التعرف على معلوماتهم الشخصية ومنها أرقام البطاقات الائتمانية واستعمالها في الشراء، ومن الأمثلة الحية عن ذلك ما حدث لسيدة أمريكية تدعى "ساندرا بوتشابين"، التي أدى تأخرها في مراجعة صندوق الرسائل الواردة إليها عبر بريدها الالكتروني، إلى أن يسرق أحدهم بطاقة ائتمانها البديلة، التي كانت قد أرسلت إليها عبر البريد الإلكتروني، ومن ثم وجدت نفسها مدينة بقيمة 1200 دولار نتيجة مشتريات قام بها أحد لصوص الهوية، الذي انتهك بريدها الالكتروني، ولم ينته الأمر عند هذا الحد، فقد قام اللص بفتح عدة حسابات جديدة باسمها لدى العديد من المحلات الأخرى، رغم أن بعض المحلات كان لديها حسابات قديمة لهذه السيدة لديها، وهذا ما جعل السيدة تتساءل عن السبب الذي حذا بهذه المحلات للموافقة على فتح حساب جديد لها، بينما يوجد لديهم حساب آخر باسمها من الأصل. يراجع: أمير فرج يوسف، المرجع السابق، ص 181-182.

تشير الإحصاءات أن حجم الخسائر الناتجة عن الاستعمال غير المشروع لبطاقات الائتمان قد بلغ في الو م أ 120 مليون دولار بين 1980-1995، لتصل الخسائر إلى 1.6 مليار دولار عام 1996، و1.64 مليار دولار عام 2002، أما البنوك البريطانية فقد تكبدت خسائر بقيمة 80 مليون جنيه إسترليني عام 1996، وقدرت خسائر البنوك الفرنسية في نهاية السنة ذاتها ما يربو عن 380 مليون فرنك فرنسي. يراجع: جهاد رضا الحباشنة، الحماية الجزائية لبطاقات الوفاء، دار الثقافة للنشر والتوزيع، عمان، الأردن2008، ص53.

بتشغيله، حيث يسأل الحامل جنائيا لمجرد امتناعه عن رد البطاقة، أو استمراره في استخدامها بعد إلغائها من البنك المصدر لها، أو استمراره في استخدامها بعد انتهاء مدة صلاحيتها".[1] وعيب على هذا التعريف أنه تناول حالة واحدة وهي استخدام البطاقة بطريقة غير مشروعة من قبل حاملها، لذلك يرى البعض أن الاستخدام غير المشروع للبطاقة يكون في كل الفروض المخالفة للاستخدام المشروع، ويكون الاستخدام مشروعا في الحالات التالية:

- إذا تم استخدام البطاقة من قبل حاملها الشرعي.
- إذا كانت البطاقة سليمة بمعنى ليست مزورة ولم يتم التلاعب بها.
- أن يتم استخدام البطاقة خلال مدة صلاحيتها، وسريانها وفي حدود ما هو مسموح به.
- أن يتم استخدام البطاقة لأجل الغرض الذي أصدرت لأجله.

وأي استخدام للبطاقة لا تتوافر فيه الشروط السابقة يخرج به من دائرة المشروعية ويضعه في دائرة اللامشروعية، وتقوم بالتالي مسؤولية الشخص الذي قام بهذا الاستخدام سواء الحامل أو الغير.[2]

بناء على ما تقدم تقوم المسؤولية الجزائية عن الاستخدام غير المشروع لبطاقات الائتمان إما من قبل حاملها أو من قبل الغير.

أولا: الاستخدام غير المشروع لبطاقة الائتمان من قبل حاملها.

يمكن للحامل أن يسيء استخدام البطاقة و يتحقق ذلك وفق عدة فروض منها: الحصول على البطاقة بمستندات مزورة، الاعتداء بالتحايل رغم صلاحية البطاقة المنتقصة، إساءة استخدام البطاقة بعد انتهاء مدة صلاحيتها، إساءة استعمال البطاقة رغم إلغاء المصدر لها، وعندما يتعلق الأمر بالسحب يمكن للحامل إساءة استخدام البطاقة بتجاوز حد السحب،[3] كما يمكن للحامل الادعاء كذبا بفقد أو سرقة البطاقة.

---

[1] أبو الوفا محمد أبو الوفا، المسؤولية الجنائية عن الاستخدام غير المشروع لبطاقات الائتمان، بحث مقدم إلى مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، المنعقد سنة 2003، كلية الشريعة والقانون، الإمارات، المجلد الخامس ص2070.

[2] د. أمجد حمدان الجهني، جرائم بطاقة الدفع الإلكتروني عبر شبكة الانترنت، بحث مقدم إلى مؤتمر المعاملات الإلكترونية المنعقد سنة 2006 بالإمارات العربية المتحدة، ص767.

[3] د. إيهاب فوزي السقا، الحماية الجنائية والأمنية لبطاقات الائتمان، دار الجامعة الجديدة، الإسكندرية، مصر 2007.

1- الحصول على بطاقة الائتمان بوثائق مزورة.

الأصل أن يتم الحصول على البطاقات طبقا للشروط والقواعد المعمول بها من قبل البنك المصدر، وحسب الوثائق المطلوبة، ولا يجوز بداهة أن يتقدم شخص لطلب البطاقة باسم أو عنوان وهمي أو ضمانات غير حقيقية.

في هذه الحالة نحن أمام فرضين: الفرض الأول أن يقوم البنك بإصدار بطاقة الائتمان اعتمادا على ما يقرره العميل طالب البطاقة، وهنا يرى الرأي الراجح في الفقه أن لا وجود لجريمة تزوير، لأن القانون يتطلب وجود محرر، ولا وجود للمحرر هنا، كما لا وجود لجريمة النصب لأن مجرد كذب صاحب الشأن بدون اقترانه بأعمال مادية أو مظاهر خارجية، لا يصل إلى مصاف الطرق الاحتيالية، وعلى البنك أن لا يعتمد فقط على أقوال العميل الشفهية، وإنما يطلب منه مستندات أو وثائق تدعم قوله.[1] أما الفرض الثاني هو أن يطلب البنك من العميل وثائق معينة كتلك التي تخص دخله الشهري أو السنوي، فيعمد العميل إلى اصطناع محرر يفيد دخله، أو يقوم بتغيير الحقيقة في الوثيقة الصحيحة المقدمة له من طرف الجهة التي يعمل بها، مما يشكل تزويرا في كلتا الحالتين، ويحاسب على جريمة الاستعمال باعتبارها جريمة مستمرة، ويحاسب على جريمة التزوير كواقعة قد تمت، وقد يحاسب على جريمة النصب لسلب ثروة الغير في الفرض الذي يقوم فيه باستعمال البطاقة للوفاء دون أن يكون له رصيد كاف في حسابه.[2]

ويرى البعض أنه حتى في حالة الحصول على بطاقة بوثائق مزورة، دون إضرار بالغير بمعنى أن يكون التزوير للحصول على البطاقة فقط، واستعمالها في حدود الرصيد المتاح ومن دون أن يلحق ذلك ضررا للبنك، فإنه في هذه الحالة لا تقوم في حق الفاعل أية جريمة، ويبقى الفيصل في الأمر وقوع الضرر من عدمه، وكذا توافر القصد الجنائي من عدمه، وتلك مسألة تخضع لتقدير القضاء.[3]

---

[1] إيهاب فوزي السقا، المرجع السابق، ص232.

[2] المرجع نفسه، ص233.

[3] المرجع نفسه، ص234.

يعتبر الحصول على البطاقات بوثائق مزورة هو الشائع، وهذا ما جعل مسؤولي "الفيزا كارد" يقولون بأن الطلبات المزورة للحصول على البطاقات الائتمانية هو الصداع الذي تعاني منه هذه الصناعة.[1]

هناك نوع آخر من الأساليب يقوم بها بعض حاملي البطاقات الملغاة في الو م أ تتمثل في ذهاب البعض إلى العصابات الإجرامية التي تطلق على نفسها عيادات الإصلاح الائتماني لتمكنهم من استخراج بطاقات ائتمان دون اعتراض البنك المصدر بعد تغيير الوثائق التي تدل على سوء استخدام العميل للبطاقة من قبل.[2]

2- الاعتداء بالتحايل رغم صلاحية البطاقة المنتقصة.

الفرض هنا أن بطاقة الائتمان استخرجت باسم صحيح، بمعنى أن البطاقة قد سلمت صحيحة من قبل البنك أو المؤسسة المالية المصدرة، إلا أن استخراج هذه البطاقة رغم صلاحيتها، قد تم بإقرار غير صحيح أو كاذب، أو أنها استخرجت بناء على مستندات مزورة بمعرفة العميل مقدم المستندات أو الوثائق، ومن مثل ذلك أن العميل يستطيع أن يوهم البنك مصدر البطاقة أن له ميزة معينة، كأن يدعي بأن دخله السنوي يفوق مبلغا معينا، والحقيقة غير ذلك، وهو ما حدث في إحدى القضايا بمصر حين ادعى أحدهم أن دخله السنوي يتجاوز 24000 جنيه، والحقيقة غير ذلك. هذه الجريمة في الفرض الأخير تكيف على أنها جريمة نصب لأن العميل اتبع طرقا احتيالية عبارة عن أكاذيب مدعمة بمظاهر خارجية،[3] كما يجوز تكييف الجريمة على أنها جريمة تزوير واستعمال مزور في حالة حصول العميل على البطاقة مع تغيير الحقيقة في الوثيقة المقدمة، كأن يقوم بكشط قيمة المبالغ التي يتقاضاها، أو وضع مبالغ أكبر تسمح له باستخراج بطاقة ذات سقف ائتماني مرتفع، ويقوم العميل بعد الحصول على البطاقة بهذه الطريقة باستخدامها في السحب أو الدفع.

تعتبر هنا البطاقة منتقصة لأنها استخرجت على غير الحقيقة، وهذا الانتقاص يتمثل في عملية التزوير الذي استخرجت بناء عليه البطاقة، فارتبطت أركان التزوير بوجود محرر، وبتغيير حقيقة

---

[1] المرجع نفسه، ص165.

[2] المرجع نفسه، ص168.

[3] إيهاب فوزي السقا، المرجع السابق، ص169-171.

ما هو مدون بالمحرر، سواء أكان التغيير كليا أم جزئيا، مع توافر احتمال الضرر الواقع على البنك كالقيام بعمليات شراء عبر شبكة الانترنت بحيث يقوم البنك بالسداد، ووجود القصد الجنائي.[1]

ويثور سؤال هنا مفاده: إذا لم يقم العميل باستخدام البطاقة وقام بإرجاعها للبنك، أو بقيت معه دون أن يستعملها حتى انتهت مدة صلاحيتها، هل يكون في هاتين الحالتين مرتكبا لجرم؟

يرى العض أن الإجابة يجب أن تكون بالنفي في كلتا الحالتين لانتفاء وقوع الضرر المتطلب لقيام جريمة التزوير، ويرى جانب من الفقه ضرورة التفرقة بين من أرجع البطاقة للبنك طواعية ومن أبقاها عنده، ففي الفرض الأول لا يؤاخذ صاحب البطاقة لأنه عدل عدولا اختياريا عن جريمته وبالتالي لا يجوز اعتبار فعله هذا شروعا في التزوير، أما من أبقى البطاقة عنده ولم يستعملها، فإنه وبالرغم من عدم تحقق الضرر للبنك لأنه لم يستخدمها، إلا أن احتمال حصول الضرر قائم، لأنه من الممكن أن تضيع منه أو تسرق وتستعمل في السحب أو الوفاء.[2]

3- الوفاء بالبطاقة مع عدم وجود رصيد كاف.

إذا قام الحامل بالوفاء ببطاقته الائتمانية الصحيحة ولكنها لم تكن تغطي قيمة المشتريات التي اقتناها، وهو يعلم أن بطاقته ليس بها رصيد كاف يلبي كل مشترياته، أو ليس بها رصيد أصلا، فهل تقوم هنا في حق الحامل جريمة؟ وإن كانت الإجابة بالإيجاب فكيف تكيف؟

تنص المواد المتعلقة بمختلف بطاقات الائتمان ومنها مثلا م9 من عقد بطاقة فيزا الصادرة عن بنك القاهرة عمان على أنه "لا يجوز للعميل (الحامل) استعمال البطاقة إلا في حدود مبلغ السقف المحدد لها، وعدم تجاوز الحدود المصرحة له من البنك، ويجوز للبنك زيادة أو تخفيض الحد عندما يشاء".[3]

انقسم القضاء الفرنسي بشأن تجاوز الحامل لرصيده في الوفاء بقيمة السلع والخدمات إلى قسمين، القسم الأول ذهب في أحكامه إلى معاقبة الحامل عن جريمة نصب، تأسيسا على أن تقديم بطاقة بدون رصيد يشكل طرقا احتيالية تهدف إلى الإقناع بوجود ائتمان وهمي، أما القسم الثاني من

---

[1] المرجع نفسه، ص236.

[2] إيهاب فوزي السقا، المرجع السابق، ص240.

[3] كميت طالب البغدادي، الاستخدام غير المشروع لبطاقة الائتمان، دار الثقافة، عمان الأردن 2008، ص144 وما بعدها.

أحكام القضاء فيميل إلى عدم مساءلة الحامل جنائيا تأسيسا على أن تسديد قيمة الفواتير مؤجل إلى حين ورود الكشف الشهري.[1]

انقسم الفقه إلى رأيين، الرأي الأول يرى عدم جواز مساءلة الحامل في هذه الحالة جزائيا، إذ أن فعله لا يعدو أن يكون إخلالا بالعقد وتعسفا في استخدام بطاقته.

أما الرأي الثاني فيذهب إلى أن فعل الحامل يشكل نشاطا إجراميا يستوجب المتابعة الجزائية، ولكن أصحاب هذا الرأي انقسموا بينهم حول التكييف القانوني للجريمة، هل هي سرقة أم خيانة أمانة أم نصب،[2] ومرد الخلاف إلى صعوبة إعمال النصوص التقليدية في قانون العقوبات، وإن كانت هنالك مسؤولية عقدية تلزم الحامل بسداد المبلغ الذي تجاوزه، ناهيك عن إمكانية توقيع جزاءات بنكية مثل سحب البطاقة أو إلغائها، وعدم السماح للحامل بالحصول على بطاقة أخرى إلا بعد مرور مدة معينة.[3]

4- إساءة استخدام البطاقة بعد انتهاء مدة صلاحيتها.

نميز هنا بين فرضين: فرض الوفاء أو الدفع بواسطة بطاقة منتهية الصلاحية، وفرض السحب بالبطاقة بعد انتهاء صلاحيتها، ففيما يخص الفرض الأول فقد انقسم الفقه بين رافض لمساءلة العميل أو الحامل للبطاقة جزائيا، وبين مؤيد لذلك، ولكل فريق من الفريقين حججه، فالفريق الرافض يرى بأن نشاط الحامل لا يشكل جريمة احتيال لانتفاء الركن المادي للجريمة، كما أن الصفة غير الصحيحة التي استعملها الحامل والتي هي ادعاؤه أنه صاحب بطاقة فاعلة، ليست هي التي دفعت البنك للوفاء، وإنما الشرط العقدي الذي يلزم البنك بذلك، ناهيك عن أن مساءلة الحامل عن جريمة الاحتيال فيه تحميل للنصوص أكثر مما تحتمل.[4]

أما الفريق الثاني فيرى أن استعمال البطاقة بعد انتهاء مدة صلاحيتها أمر غير مشروع، يشكل الركن المادي لجريمة الاحتيال، ذلك أن حامل البطاقة أراد أن يظهر باعتباره صاحب صفة

---

[1] رضا أحمد إبراهيم محمود عيد، الأحكام الموضوعية والإجرائية للجرائم الناشئة عن استخدام بطاقة الائتمان، رسالة لنيل درجة دكتوراه في الحقوق، تخصص القانون الجنائي، جامعة عين شمس، مصر (دون ذكر تاريخ المناقشة)، ص ص94-95.

[2] كميت طالب البغدادي، المرجع السابق، ص146.

[3] رضا أحمد، المرجع السابق، ص98.

[4] الحباشنة، المرجع السابق، ص130.

(غير حقيقية) تهدف إلى إقناع المجني عليه بوجود ائتمان لا وجود له في الواقع، خاصة وأن انتهاء صلاحية البطاقة يخلع عنها قيمتها كأداة ائتمان.

وذهب أيضا إلى أن الحامل الذي يعلم بأن البطاقة منتهية الصلاحية أو ملغاة، ورغم ذلك يتقدم إلى التاجر لسداد قيمة تعاملاته، يكذب ويستعمل إحدى وسائل الاحتيال، ألا وهي إبراز مستندات منسوبة للغير، للتوصل من خلال ذلك إلى إيهام التاجر بأنه ما زال دائنا بضمان قبول البطاقة استنادا إلى العقد المبرم بينه وبين البنك.[1]

ولكن، ما موقف التاجر من قبول البطاقة منتهية الصلاحية؟

يفرق غالبية الفقه والقضاء بين عدة حالات:[2]

الحالة الأولى: قيام الحامل خطأ باستخدام البطاقة منتهية الصلاحية، في حين يحتفظ برصيد لدى البنك.

في علاقة التاجر بالبنك، يعد التاجر الذي يقبل الوفاء ببطاقة منتهية الصلاحية مرتكبا خطأ وإخلالا في العقد المبرم مع البنك، وعليه تحمل خطئه، ويمتنع البنك عن دفع قيمة الفواتير إلى التاجر .

في علاقة التاجر بحامل البطاقة، فعلى التاجر التحقق من شخصية حامل البطاقة، وفي حال وقوع خطأ فعلى الحامل أن يوفي إلى لتاجر عند رفض البنك الوفاء إلى التاجر.

في علاقة الحامل بالبنك، إذا اعترف الحامل بأنه هو القائم بالعمليات المنفذة، فلكل من البنك أو التاجر الحق في الرجوع على الحامل بالوفاء.

الحالة الثانية: اتفاق التاجر مع الحامل على قبول الوفاء بالبطاقة منتهية الصلاحية إضرارا بالبنك، فهنا تتوافر الطرق الاحتيالية اللازمة لقيام جريمة النصب، ويسأل الحامل باعتباره فاعلا ويسأل التاجر باعتباره شريكا.

---

[1] الحباشنة، المرجع السابق، ص131.

[2] المرجع نفسه، ص ص131-132.

الحالة الثالثة: قيام الحامل باستخدام البطاقة منتهية الصلاحية للوفاء، في حين أنه لا يملك حسابا بنكيا، وينكر أيضا أنه القائم بهذه العمليات، في هذه الحالة يكون الحامل قد استخدم طرقا احتيالية، وصفة غير صحيحة وتقوم بذلك في حقه جريمة النصب (الاحتيال). ويرى البعض بأنه من الصعوبة بما كان إثبات أن الحامل كان سيء النية عند استخدام البطاقة منتهية الصلاحية، وعلى فرض ثبوت سوء نيته فلا يجوز مساءلته إلا مدنيا لإخلاله بالتزام عقدي. ونتفق مع أصحاب هذا الرأي في أن إثبات سوء نية الحامل أمر بالغ الصعوبة، ولكن في حال تم ذلك فما المانع من مساءلته جزائيا؟ صونا للمصلحة القانونية المحمية هنا وهي الثقة في البطاقة الائتمانية.

أما الفرض الثاني وهو قيام الحامل باستخدام البطاقة منتهية الصلاحية في سحب النقود، فيذهب جانب من الفقه أن هذا الفعل لا يشكل جريمة لوجود استحالة مادية متمثلة في قيام جهاز الصرف النقدي بابتلاع البطاقة أو رفضها عند إدخالها، إلا أن جانبا من الفقه يرى بأنه في حالة تمكن الحامل من سحب الأوراق النقدية من الجهاز باستخدام بطاقة منتهية الصلاحية بعد إدخال رقم سري خاص بها أو بأخرى بحيث لم يقم الجهاز بسحب البطاقة أو رفضها فإن الحامل هنا يعد مرتكبا جريمة النصب باستعمال الطرق الاحتيالية.[1] وهذا ما ذهبت إليه محكمة جنح"Angers" الفرنسية، ورأى جانب من الفقه أن الفعل يعتبر خيانة أمانة، باعتبار أن البطاقة أمانة عند حاملها على سبيل الوديعة، ويجب ردها للبنك بعد انقضاء صلاحيتها، ويرى فريق ثالث من الفقه أن الفعل لا يشكل جريمة أصلا سواء تمكن الحامل من السحب أو الوفاء بالبطاقة منتهية الصلاحية لأن ذلك يرجع إلى البنك الذي سمح له بالموافقة على التعامل بالبطاقة، إلا في حالة التلاعب في بيانات البطاقة ذاتها للحصول على أموال خاصة بالغير، فهنا يسأل الحامل جزائيا وفق نصوص التزوير.[2]

5- إساءة استخدام البطاقة رغم إلغاء المصدر لها.

قد تقوم الجهة مصدرة للبطاقة بإلغائها، لأي سبب من الأسباب، كأن يكون الحامل أساء استخدامها، أو أن تتدخل ظروف تطال المركز المالي للحامل بحيث تؤثر سلبا في اعتباره الشخصي،[3] وتنص غالبية العقود الخاصة بالبطاقات الائتمانية على حق البنك في أن يوقف استخدام

---

[1] الحباشنة، المرجع السابق، ص134.

[2] السقا، المرجع السابق، ص174، ويراجع أيضا: محمد نور الدين، المرجع السابق، ص214.

[3] نضال سليم برهم، أحكام عقود التجارة الالكترونية، الطبعة الأولى، الإصدار الثاني، دار الثقافة، عمان، الأردن 2009، ص156.

البطاقة كليا أو جزئيا، أو إلغاء البطاقة في أي وقت ودون إخطار.[1] كما يجوز لحامل البطاقة طلب إلغائها وفق إجراءات معينة مع التزامه برد البطاقة.[2]

ويتوجب في هذه الحالة على البنك المصدر تنبيه الحامل ومطالبته برد البطاقة، فإذا لم يقم الحامل برد البطاقة واستعملها ترتب عن ذلك أمران: الأول أن يقوم البنك بإخطار التاجر بإلغاء البطاقة، وهنا يتوجب على التاجر عدم قبولها في التعامل، وفي حالة إهماله يتحمل تبعات ذلك، ولا تقوم – حسب الفقه الراجح – بحق الحامل جريمة النصب، رغم أن محكمة باريس قضت في حكم لها بأن سلوك الحامل بعدم رد البطاقة رغم إلغائها يعد من قبيل الطرق الاحتيالية التي هدفها الإقناع بوجود ائتمان (وهمي)،[3] إلا أن بعض الفقه يرى أن الحامل يحاسب هنا على جريمة خيانة الأمانة، كونه قد عبر عن تغيير نيته باختلاس البطاقة لنفسه إضرارا بالجهة المالكة لها[4]؛ أما الأمر الثاني فهو عدم إخطار البنك المصدر التاجر بإلغاء البطاقة، وقيام الحامل باستخدامها في الوفاء وهو يعلم أنها ملغاة، هنا يرى جانب من الفقه أن الحامل قد أو هم التاجر بقانونية البطاقة ووجود الائتمان، مما دفعه إلى قبولها، فيكون الحامل بهذا الفعل مرتكبا لجريمة النصب،[5] وهو ما أيده القضاء، خاصة وأن إلغاء البطاقة يخلع عنها قيمتها كأداة ائتمان، مما يشكل فعل الوفاء بها استيلاء على ثروة الغير، كما أن تقديم البطاقة الملغاة للوفاء يعد استعمالا لصفة غير صحيحة، ولن يستطيع التاجر اكتشاف إلغاء البطاقة إلا من خلال الوسائل الموضوعة تحت تصرفه، وهي القائمة السوداء، أو الاتصال بمركز الإذن في حالة ما إذا تجاوزت قيمة النفقات الحد الأقصى لقيمة البطاقة.[6]

وذهب بعض الفقه إلى أن استخدام البطاقة بعد إلغائها يعتبر شروعا في السرقة، وذلك لأن إلغاء البطاقة تم بسبب عدم وجود رصيد.[7]

---

[1] محمد نور الدين، المرجع السابق، ص157.

[2] المرجع نفسه، ص158.

[3] رضا أحمد إبراهيم محمود عيد، المرجع السابق، ص101.

[4] المرجع نفسه، ص101.

[5] نضال سليم برهم، المرجع السابق، ص157.

[6] رضا أحمد إبراهيم محمود عيد، المرجع السابق، ص102.

[7] السقا، المرجع السابق، ص176.

أما استخدام البطاقة الملغاة في السحب من الموزع الآلي، فيرى البعض أنه لا يشكل جريمة، ويرى البعض الآخر أنها تمثل جريمة الشروع في السرقة إذا لم ينجح في تحقيق النتيجة، وسرقة إذا تمكن من الحصول على النقود، وذهب البعض إلى أن استعمال البطاقة الملغاة في السحب تقوم به جريمة النصب باستخدام صفة غير صحيحة.[1]

6- إساءة استخدام البطاقة بتجاوز حد السحب

المفروض أن حد السحب يقف عند مبلغ معين يتحدد عند تعاقد الحامل مع البنك، فلا يجوز استخدام البطاقة في السحب إلا إذا كان هناك رصيد كاف يسمح بذلك، ولكن قد يقوم الحامل بتجاوز حد السحب بسوء نية، سواء باستخدام طرق احتيالية أو بالتواطؤ مع موظف البنك أو مع التاجر. وقد اختلف الفقه والقضاء حول تكييف هذه الاعتداءات، هل هي جرائم سرقة أم نصب أم خيانة للأمانة ؟ واكتفت محكمة النقض الفرنسية في بعض القضايا المعروضة عليها بالمسؤولية العقدية لحامل البطاقة، بمعنى أنها استبعدت المسؤولية الجزائية للحامل.[2]

قد يكون لهذا الأمر الكثير من المبررات التي تدعمه، منها أن تجاوز الحامل لرصيده بالسحب باستخدام بطاقته وفقا لنظام تشغيل الجهاز الآلي، يؤدي مباشرة إلى تسجيل القيمة الزائدة في الجانب المدين من حساب الحامل، ويبقى الحامل مطالبا بتلك القيمة على أساس أنه مدين بها وليس سارقا لها.[3]

وقد حكمت محكمة النقض الفرنسية بمناسبة الطعن المقدم ضد محكمة استئناف "Angers" بتاريخ 1982/02/04 في قضية "Lafont" بقولها: "السحب من الموزع الآلي للأوراق النقدية من البنك بواسطة حامل البطاقة لمبلغ من النقود يتجاوز الرصيد الدائن في حسابه المصرفي لا يفسر إلا على أنه عدم احترام أو مراعاة الالتزام التعاقدي ولا يندرج تحت أي نص عقابي".[4]

---

[1] رضا أحمد إبراهيم محمود عيد، المرجع السابق، ص103.

[2] المرجع نفسه، ص179-181.

[3] أمينة بن عيمور، البطاقات الالكترونية للدفع والقرض والسحب، مذكرة ماجستير في القانون الخاص، تخصص قانون أعمال، جامعة منتوري، قسنطينة، 2005/2004، ص129.

[4] محمد نور الدين، المسؤولية الجنائية... المرجع السابق، ص117.

غير أن بعض الفقه المصري ينتقد حكم محكمة النقض الفرنسية السابق، باعتباره جاء مخالفا للاتجاه العام الذي يسود جميع أحكامها، فيما يتعلق بتطبيقها معيارا واسعا في مجال الاختلاس، منذ بداية القرن العشرين، باعتناقها المفهوم القانوني للاختلاس الذي يهتم أساسا بفكرة اغتصاب حيازة الشيء من صاحبه، أكثر مما يهتم بفكرة الاغتصاب المادي له، وهي قوام المفهوم المادي للاختلاس.[1]

يرى جانب من الفقه الفرنسي والمصري، أن تجاوز الحامل للسحب عن طريق بطاقته الائتمانية، يجوز أن تطبق عليه المواد المتعلقة بجريمة الدخول غير المشروع إلى نظم المعالجة الآلية للمعطيات، أو نصوص الاعتداء العمدي على المعطيات المعالجة آليا.[2]

قد يقوم حامل البطاقة باستخدام خدمات نقاط البيع الالكترونية في إيداع شيكات بدون رصيد، بحيث تضاف قيمة الشيك إلى قيمة الحساب الأصلي، ثم يلجأ الحامل لتحصيل قيمة هذه الشيكات بواسطة نقاط البيع الإلكترونية قبل إجراء المقاصة بين البنوك بعضها بعضا. ويشكل هذا الأمر جريمتين، الأولى هي جريمة إصدار شيك من دون رصيد، والثانية هي جريمة نصب تقع بأسلوب التحايل بصرف القيمة دون أن تتم المقاصة بين البنوك، أي قبل أن يكتشف البنك المصدر ذلك.

نظرا لاختلاف التوصيفات في جرائم بطاقات الائتمان، فإنه بات من الضروري استصدار تشريعات خاصة تغطي كافة احتمالات الاعتداء التي يمكن أن تكون البطاقات محلا لها، لتجنب الأحكام المتضاربة للقضاء نتيجة الاجتهادات في توصيف الجرائم.[3]

7- استعمال البطاقة المعلن كذبا بسرقتها أو فقدها.

فقد البطاقة أو سرقتها أمر بالغ الخطورة، فهو نقطة بداية في سلسلة العمليات غير المشروعة الواقعة عليها من طرف من استحوذ عليها، ولذا فإن من أهم التزامات الحامل المحافظة عليها وعلى رقمها السري، كما يتوجب على الحامل القيام بالمعارضة فور اكتشافه اختفاء بطاقته أو رقمه السري، وهذا ما نجده مثلا التوجيه الأوربي الصادر في 17 نوفمبر 1988 حيث نصت م1/4 منه

[1] محمد نور الدين، المرجع السابق، ص122.

[2] المرجع نفسه، ص126.

[3] المرجع نفسه، ص181.

على: "يجب أن تفرض الشروط التعاقدية على الحامل في مواجهة المصدر الالتزام بإعلام المصدر أو المركز الرئيسي – دون تأخير كبير–[1] بعد التحقق من سرقة أو فقد أو تزوير وسيلة الوفاء أو طريقة استخدامها".[2] وتجيز بعض البنوك أن تكون المعارضة شفاهة، على أن يعزز الحامل معارضته بطلب مكتوب خلال مدة معينة.

دفع تعدد الغش والاحتيال باستعمال البطاقات البنكية، خاصة عن طريق استخدامها في الوفاء عبر شبكة الانترنت، المشرعَ الفرنسي إلى إصدار قانون خاص لمعالجة هذا الموضوع، وهو القانون رقم 1062-2001 الصادر في 15 نوفمبر 2001 والخاص بالأمان اليومي "Sécurité quotidienne" وقد أضاف هذا القانون حالة معارضة جديدة خاصة باستعمال البطاقة عن طريق الغش "Utilisation frauduleuse de la carte" وحدد المسؤولية إلى حد أعلى 400 يورو، وشريطة ألا يرتكب الحامل خطأ جسيما، وألا يهمل في إجراء المعارضة بمعنى أن يقوم بالمعارضة في أفضل المهلات، مع مراعاة عاداته في استخدام البطاقة،[3] وتم إرجاع هذا الحد إلى 275 يورو في فاتح يناير 2002، و150 يورو في فاتح يناير 2003، بل أعفى القانون حامل البطاقة من كل مسؤولية في حالة الوفاء الذي يتم عن طريق الغش عن بعد، دون استخدام مادي للبطاقة، وفي حالة الوفاء الذي يتم بتقليد البطاقة، وفي لحظة العملية كانت البطاقة في حوزة الحامل المادية.[4]

في الحالة محل البحث، يقوم الحامل بكل ما يجب عليه عمله في حالة سرقة أو فقد البطاقة، إذ يعلم البنك المصدر أو الشرطة بفقد أو سرقة بطاقته، في حين أنها لا تزال معه، ويستعملها في السحب أو الوفاء، ويطلق بعض الفقه على هذه الحالة مصطلح السرقة الصورية، تمييزا لها عن السرقة الحقيقية أي الاختلاس الحقيقي للبطاقة، وهدف الحامل من هذه المعارضة الكاذبة هو الاستفادة من الإعفاء من المسؤولية عن فقد أو سرقة البطاقة من تاريخ المعارضة، حيث يسارع

[1] في دعوى لم يقم فيها الحامل بإجراء المعارضة إلا بعد أسبوع من السرقة، أدانت محكمة فرنسية هذا الحامل، وأكدت محكمة النقض هذه الإدانة، حيث أعلنت أنه: "في حالة سرقة بطاقة زرقاء، فإن الشخص الذي كان حاملا لها، والذي وقع بإمضائه على الشروط التعاقدية المتعلقة باستخدام البطاقة، خصوصا في حالة الفقد أو السرقة، واستخدام الغير لهذه البطاقة بشكل احتيالي، فإنه يكون بريئا من المسؤولية من اللحظة التي قام فيها بتنبيه البنك المصدر للبطاقة، غير أن هذا الشخص قد قبل خطر الاستعمال الاحتيالي أو التدليسي للبطاقة الزرقاء بالنسبة للفترة السابقة على المعارضة فيها، وأن مسؤوليته كانت ملتزمة وقت إجرائه إياها". محمد نور الدين، المرجع السابق، ص226.

[2] المرجع نفسه، ص219.

[3] المرجع نفسه، ص222.

[4] المرجع نفسه، ص223.

باستخدام البطاقة في السحب قبل قيام البنك بمحو البرمجة الخاصة بالموزعات أو أجهزة السحب النقدي الآلي، أو في الوفاء حيث لا يمكن اكتشاف الغش إلا بعد فترة عن طريق المواجهة بين التاجر والحامل.[1] ويرى أغلب الفقه أن الحامل قد فقد صفته كحامل شرعي للبطاقة، مما يجعل من الواجب اعتباره من الغير ابتداء من لحظة المعارضة،[2] لذا فإن أي استعمال للبطاقة بعد هذه اللحظة يعتبر استعمالا غير مشروع للبطاقة من قبل الغير، وعلى ذلك يجوز تكييف فعل الحامل الذي أصبح من الغير على أنه يكوّن جريمة نصب، باعتباره يكون قد تحايل لإجبار البنك على الوفاء للتاجر، إذ تقوم الطرق الاحتيالية بوضوح، خاصة وأنها مدعمة بالإخطار الكاذب بفقد أو سرقة البطاقة، وهو ما تقوم به جريمة النصب، وهذا ما قضت به محكمة النقض الفرنسية حيث أعلنت توافر جريمة النصب في حق متهم ادعى كذبا بفقد بطاقتين له في إفريقيا وألمانيا على التوالي، وقام بعد ذلك باستخدامهما.[3]

ومن الفقه من يرى أن فعل الحامل في هذا الفرض تنطبق عليه نصوص خيانة الأمانة، إذ أن الادعاء بفقد أو سرقة البطاقة يكفي لتحقق الاختلاس، واستعمالها بعد ذلك يعتبر تجريدا لها من قيمتها، ويسبب ذلك كله ضررا للبنك المصدر للبطاقة، كما يذهب البعض إلى القول بوجود تعدد الجرائم، حيث توجد جريمة تزوير الإعلانات، تأخذ صورة التزوير المعنوي أي جعل واقعة مزورة أو غير صحيحة محل صورة واقعة صحيحة بالنسبة لإعلان الحامل كذبا بفقد أو سرقة البطاقة.[4]

وتكمن صعوبة اكتشاف الجريمة في هذه الحالة في عدم وجود نظام للتحقق رسميا من القائم بعملية الشراء من التاجر، فليس ثمة دليل قاطع يجوز التمسك به ضد الحامل،[5] بمعنى أن الحامل يدعي أنه ليس هو من قام باستخدام البطاقة، وهذا يؤدي إلى الشك الذي يفسر لصالحه.

ثانيا: الاستخدام غير المشروع لبطاقة الائتمان من قبل الغير.

يقصد بالغير هنا، كل شخص آخر غير الحامل الشرعي للبطاقة؛ والذي قد يلجأ إلى تزوير بطاقة الائتمان أو إلى استعمال بطاقة مزورة، كما قد يقوم بسرقة هذه البطاقة، ولتجنب خطر

---

[1] محمد نور الدين، المرجع السابق، ص ص225-227.

[2] رضا أحمد إبراهيم محمود عيد، المرجع السابق، ص117.

[3] المرجع نفسه، ص118-119.

[4] محمد نور الدين، المرجع السابق، ص ص231-234.

[5] رضا أحمد إبراهيم محمود عيد، المرجع السابق ، ص118.

الاستعمال غير المشروع للبطاقة من قبل الغير، فإن الحل الأكثر عقلانية للحامل هو القيام بعملية التأمين ضد فقد أو سرقة البطاقة، وغالبا ما تقوم البنوك المصدرة للبطاقة بضمان هذه العملية للحامل إن شاء ذلك، ولكن هذا الأمر لا يعني أن الحامل لا يلتزم مبدأ الحذر، ومعناه الحرص على بطاقته والمعطيات التي عليها، ومراقبة عمليات الدفع والسحب عن طريق الاهتمام بمطاعة الكشوفات التي يقوم البنك بإرسالها دوريا.[1]

1- إعتداء الغير على بطاقة الائتمان عن طريق تزويرها.

قد يفقد الحامل بطاقته أو تسرق منه، فيستعملها الغير في الشراء أو السحب بعد أن يستبدل ما بها من بيانات ومعلومات. ويشكل هذا الأمر اعتداء على البنك مصدر البطاقة وعلى حاملها الشرعي، فهل يعد هذا الاعتداء على البطاقة جريمة تزوير لأنه تغيير للحقيقة؟[2]

الإجابة عن هذا التساؤل تقتضي الإجابة عن السؤال التالي:

إلى أي مدى يجوز اعتبار البطاقة محررا بالنسبة للبيانات المرئية المدونة عليها؟ وهل البيانات المدونة إلكترونيا على البطاقة تعتبر من قبيل المحرر الذي يمكن أن يكون محلا للتزوير؟

من خلال التعريفات المختلفة المقدمة للمحرر، فإن الفقه يكاد يجمع على أن البيانات المكتوبة بصورة مرئية بحروف بارزة على البطاقة تعتبر محلا لجريمة التزوير، لأنه تتوفر فيها مقومات المحرر، مهما كانت اللغة الصادرة بها البطاقة، أو الطريقة التي دونت بها الحروف على البطاقة، أو المادة المستخدمة في الكتابة، فبمجرد الإطلاع على البطاقة يستطيع كل المتعاملين بنظام الوفاء بالبطاقات تحديد كون مقدم البطاقة هو حاملها الشرعي أم لا، ما دامت البطاقة صحيحة لا يشوبها عيب أو تشويه.[3]

وإذا لم يكن هنالك خلاف حول البيانات المرئية المدونة على البطاقة، فإن البيانات الإلكترونية أثارت حفيظة بعض الفقه الذي اعتبر البيانات المخزنة في الأشرطة الممغنطة لا تشكل كتابة، وعليه لا يجوز حسبهم القول بالتزوير، وهذا ما أكده أيضا بعض الفقه الألماني، وكذا الرأي

[1] JeanStouflet, instruments fe paiment et de crédit, 8ème édition, LexisNexis, Paris 2012, p 455.

[2] الحباشنة، المرجع السابق، ص60. السقا، المرجع السابق، ص188.

[3] محمد نور الدين، المرجع السابق، ص89.

السائد في الفقه المصري والذي يؤكد على أن الكتابة من مثل هذه الدعامات لا تتمتع بخاصية الدوام النسبي، إذ يمكن تعديلها في أي لحظة دون أن تترك أي أثر مادي يدل عليه، وعليه لا يجوز أن ينطبق عليها وصف المحرر، إذ لا يتداولها الناس فيما بينهم، وعليه فإن التلاعب في البيانات المخزنة على الأشرطة الممغنطة قد تقوم به جريمة الإتلاف أكثر منها جريمة التزوير.[1]

وذهب جانب من الفقه المصري خلاف هذا الأمر، واعتبر أن البيانات المسجلة بطريقة إلكترونية تعتبر من قبيل الكتابة التي يمكن أن تقع جريمة التزوير عليها إذا توافرت بقية أركانها، إذ أن قانون العقوبات لم يحدد المقصود بالمحرر، ولا يجوز أن يقف حجر عثرة أمام المستجدات الفنية الجديدة، إذ من شأن ذلك زعزعة الثقة في مثل هذه المحررات خاصة بعد تعاظم الاعتماد عليها، كما أنه لم يقل أحد بأن إخفاء معنى المحرر عن العين المجردة، واحتياجه لإجراءات خاصة ينفي وجوده.[2]

غير أن المشرع الفرنسي من خلال مجموعة من القوانين منها القانون رقم 19 لسنة 1988 الخاص بالجرائم المعلوماتية أو ما يصطلح عليه بعض الكتاب الغش المعلوماتي، " la fraude informatique"، وقانون العقوبات الجديد لسنة 1994، والقانون الخاص بتأمين الشيكات وبطاقات الوفاء الصادر في 30 ديسمبر 1991 قطع كل خلاف حول مدى اعتبار البطاقات من قبيل المحررات، بحيث لم يعد هنالك خلاف حول اعتبارها محررات يمكن أن يقع التزوير عليها.[3]

ومن خلال نصوص هذه القوانين يتضح أن المشرع الفرنسي لم يخرج عن المبدأ العام في جرائم تزوير المحررات واستعمالها، حيث فصل بين جريمة تزوير البطاقة وجريمة استعمال بطاقة مزورة، وأن عدم استعمال بطاقة مزورة لا يمنع من عقاب المزور، وعدم عقاب من قام بفعل التزوير لا يمنع من معاقبة من قام مرتكب فعل الاستعمال، متى كان عالما بأنه يستعمل بطاقة مزورة.[4]

---

[1] المرجع نفسه، ص94.

[2] المرجع نفسه، ص100.

[3] المرجع نفسه، ص96.

بهذا الخصوص صدر حكم من محكمة النقض الفرنسية في 21 فبراير 1995، اعتبرت فيه الشريط الممغنط وما يحوي من معلومات ظاهرة من قبيل المحررات حتى ولو اقتضى هذا المحرر وبشكل حديث جهازا ملائما لقراءته واستيضاح دلالاته؛ وبناء عليه رفضت المحكمة الطعن المقدم ضد حكم محكمة استئناف (روان) التي أدانت المتهم بجريمة تزوير في المحررات الخاصة، لقيامه بنسخ المعلومات الظاهرة على الأشرطة الممغنطة للبطاقات المسروقة على بطاقات فارغة. المرجع نفسه، ص99.

[4] الحباشنة، المرجع السابق، ص83.

تزوير بطاقات الائتمان قد يكون كليا وقد يكون جزئيا، سواء في بيانات البطاقة أو في البيانات المدونة إلكترونيا، ولا يأل المزورون جهدا في ابتكار وسائل حديثة ومتطورة للقيام بعمليات التزوير، وتعتبر هونغ كونج المركز الرئيس لعمليات تزوير البطاقات.[1]

ومن الطرق التي يلجأ إليها مزورو البطاقات الاختراق غير المشروع لمنظومة خطوط الاتصالات العالمية بما تشتمل من حاسبات آلية وبرامج وشبكات اتصال، كما يستعملون تقنية تفجير الموقع المستهدف عن طريق ضخ مئات الآلاف من الرسائل الإلكترونية أو رسائل البريد الإلكتروني إلى جهاز الضحية والذي غالبا ما يكون بنكا أو مؤسسة مالية أخرى أو فندقا... للتأثير على ما يعرف بالسعة التخزينية للموقع المستهدف بحيث يشكل ذلك ضغطا يؤدي إلى تفجير الموقع العامل على الشبكة، وما يستتبع ذلك من تشتيت المعلومات والبيانات المخزنة فيه يسهل مع هذا الأمر للمجرم المعلوماتي الحصول عليها أو على الأقل التجول أو الحركة في موقع الضحية بسهولة والحصول على كل ما يحتاجه من معلومات وبيانات وأرقام خاصة بالبطاقات الائتمانية للغير.

كما يلجأ البعض إلى أسلوب التجسس، عن طريق استخدام البرامج التي تمكنهم من الإطلاع على البيانات والمعلومات الخاصة بالغير وخاصة الشركات الكبرى، بهدف الحصول على أرقام بطاقات ائتمان المتعاملين معها بغية استعمالها بطريقة غير مشروعة، كما يقومون باستعمال أسلوب الخداع، ويتحقق ذلك بإنشاء مواقع وهمية على شبكة الانترنت على غرار المواقع الأصلية، ولكي يتم ذلك يقوم القراصنة بالحصول على كافة بيانات الموقع الأصلي وإدخال تعديلات عليه لكي لا يظهر أن هناك ازدواجا في المواقع، وتبعا لذلك يستقبلون كافة المعاملات التجارية الخاصة بالموقع الأصلي، والتي سيكون من بينها بيانات البطاقات الائتمانية، وهذا الأمر يضر المواقع الأصلية وأصحاب البطاقات الائتمانية، ويهز ثقة المتعاملين في التجارة الالكترونية، كما قد يلجأ البعض إلى ما يسمى تخليق أرقام البطاقات عن طريق مجموعة من المعادلات الرياضية والإحصائية.[2]

هذه الأساليب تعتبر تهديدا حقيقيا للتجارة الإلكترونية، باعتبارها تهدد وسيلة الدفع الأولى المستخدمة في هذه التجارة، ويدل على ذلك أن محصلة المشتريات بواسطة البطاقات الائتمانية

[1] السقا، المرجع السابق، ص192.

[2] بيومي حجازي، الحماية الجنائية...الكتاب الأول، مرجع سابق، ص131-134.

المسروقة يقارب 110 مليون دولار أسبوعيا، مما دفع البنوك إلى إصدار بطاقة خاصة بالتسوق عبر الانترنت يوضع بها مبلغ معين من المال يكون في الغالب بسيطا، بحيث إذا ما التقطت أرقامها، واستعملت عن طريق القراصنة كانت الخسارة محدودة.[1]

2- إعتداء الغير بسرقة أموال البطاقة الائتمانية.

من الاعتداءات التي تقع على البطاقة الائتمانية سرقة البطاقة ذاتها، وهنا لا خلاف على انطباق نصوص جريمة السرقة، باعتبار البطاقة محلا لحقوق مالية مملوكة للغير، سواء استعمل السارق البطاقة أم لم يستعملها، كأن تكون نية الفاعل مجرد الاحتفاظ بها وحرمان صاحبها من استعمالها،[2]ولا يؤثر عدم معرفة السارق لرقم البطاقة السري، لأن شأنها في ذلك شأن الشيكات غير الموقع عليها، إذ من الممكن أن تكون محلا للاختلاس وإن كانت قليلة القيمة في ذاتها، إلا أنها ليست مجردة من كل قيمة، فتفاهة القيمة وإن اعتبرت من أسباب التخفيف، إلا أنها لا تنفي الجريمة المرتكبة وهي السرقة، أو النصب كما ذهب إليه جانب من الفقه.[3]

بيد أن السؤال التالي يطرح نفسه: ما حكم من عثر على بطاقة ولم يردها إلى صاحبها؟ بل استعملها في الوفاء أو السحب؟ هل تنطبق عليه جريمة السرقة؟

للوهلة الأولى يبدو أنه لا يجوز مساءلة الشخص الذي عثر على البطاقة لانتفاء الركن المعنوي لديه وهو نية التملك، كما أنه لم يقم باختلاس البطاقة، إلا أن جانبا كبيرا من الفقه يرى ضرورة التفرقة بين حالة الاستعمال دون وجه حق وحالة تجريد البطاقة من قيمتها كليا أو جزئيا ثم ردها بعد ذلك إلى حاملها الأصلي، ففي حالة تجريد البطاقة من كل أو بعض قيمتها تقوم جريمة السرقة حسب الرأي الراجح، ويرى البعض أن الجريمة عبارة عن نصب لأن الفعل الإجرامي للجاني يشكل وسيلة من الوسائل الاحتيالية التي تقوم بها جريمة النصب، ويرى البعض أنه في حالة استعمال

[1] السقا، المرجع السابق، ص205.

[2] المرجع نفسه، ص193.

[3] معادي أسعد محمد صوالحة، بطاقات الائتمان، النظام القانوني وآليات الحماية الجنائية والأمنية، دار الآفاق المغربية للنشر والتوزيع، الرباط، المغرب 2008، ص349.

البطاقة للوفاء فإن الجاني يسأل عن جريمة التزوير، باعتباره قد قلد توقيع حامل البطاقة على الأوراق الخاصة بعملية البيع.[1]

وتتم السرقة عن طريق الطرق التقليدية المعروفة أو عن طريق وسائل مبتكرة، ومن ذلك ما قامت به إحدى العصابات في الو م أ من صنع آلة سحب آلي ووضعها في أحد الشوارع العامة، وحينما يتقدم حامل البطاقة من الآلة لسحب النقود يفاجأ عند إدخاله البطاقة والرقم السري بابتلاع الآلة للبطاقة وتظهر له عبارة راجع بنكك، فيغادر مكان الآلة؛ بعد ذلك تحصل العصابة على البطاقة والرقم السري، وتستخدمها في الاستيلاء على أمواله من البنك المصدر، وتستخدم هذه الطريقة أيضا بفرنسا وتعتبر أكثر الطرق إزعاجا للبنوك الفرنسية، حيث قرر أن هنالك 300 عصابة تستخدم هذا الأسلوب بمعدل ثلاثين حالة أسبوعيا.[2]وهناك طرق أخرى من بينها سرقة المعلومات الخاصة بالبطاقات من خلال أجهزة الحاسب الآلي الخاص بالبنك المصدر للبطاقة، بل أن هناك من قام بسرقة آلة السحب ذاتها بما تحويه من أموال وبطاقات.[3]

3- إعتداء الغير بالاحتيال للاستيلاء على أموال بطاقات الائتمان.

هناك العديد من الأمثلة عن احتيال الغير للحصول على معلومات حول بطاقة الائتمان، منها الاتصال بالحامل وإخباره أنه فاز برحلة مجانية، والطلب منه تبعا لذلك بعض المعلومات ومنها رقم بطاقته الائتمانية، أو يتصل أحدهم بالحامل وإخباره أنه موظف البنك المصدر للبطاقة ويحتاج إلى بعض المعلومات، وبعد ذلك تستغل تلك المعلومات والبيانات في الحصول على الأموال باستخدام بيانات هذه البطاقات.[4]وطرق الاحتيال كثيرة، وكل يوم يفاجئنا القراصنة بأساليب جديدة، ولا شك أنها تخضع كلها لما هو مقرر في جريمة النصب.

الفرع الثالث: الحماية الجزائية للتوقيع الإلكتروني

بالرغم من أهمية التدابير الوقائية للحد من ارتكاب الجرائم الناشئة بسبب موضوع التوقيع الإلكتروني، إلا أن هذه التدابير ومهما بلغت من دقة لن تؤدي إلى الحد من ارتكاب تلك الجرائم

---

[1] معادي أسعد محمد صوالحة، المرجع السابق، ص ص351-352.

[2] السقا، المرجع السابق، ص194

[3] المرجع نفسه، ص196.

[4] السقا، المرجع السابق، ص197.

بصفة مطلقة، لذلك بات لزاما على مختلف التشريعات تنظيم الجزاءات الجنائية لإسباغ حماية إضافية وفعالة للتوقيعات الإلكترونية.[1]

ويثير موضوع الحماية الجزائية للتوقيع الإلكتروني والجرائم التي تمثل اعتداء عليه العديد من المسائل القانونية، المتعلقة بالعقود الإلكترونية والتجارة الإلكترونية وغيرها، كما يثير من الناحية العملية الكثير من الصعوبات تتمثل خاصة في اختراق نظم المعلومات، وعدم الثقة في استخدام شبكة الانترنت في المعاملات، وتوسع البنوك في الاعتماد على المعاملات الإلكترونية، وأساليب الحماية الإلكترونية.[2]

من أهم المصالح المحمية من إرساء الحماية الجنائية للتوقيع الإلكتروني حماية شرعية تداول البيانات، وسرية البيانات وخصوصيتها، وحماية المستهلك الإلكتروني من الغش والتحايل، وإعطاء الثقة في التوقيع الإلكتروني.[3]

لإجلاء الغموض عن هذا الموضوع، نتطرق أولا إلى ماهية التوقيع الإلكتروني، ثم إلى مختلف الاعتداءات الواقعة عليه.

أولا: ماهية التوقيع الإلكتروني.

يتم التطرق إلى التوقيع الإلكتروني وشروطه، ثم إلى صوره.

1- تعريف التوقيع الإلكتروني وشروطه.

يعرف الفقه التوقيع بأنه التأشير أو وضع علامة على السند، أو بصمة إبهام، للتعبير عن القبول بما ورد فيه، أو أنه أية علامة مميزة وخاصة بالشخص الموقع تسمح بتحديد شخصيته والتعرف

[1] د. أيمن رمضان محمد أحمد، الحماية الجنائية للتوقيع الإلكتروني، دار النهضة العربية، القاهرة 2011، ص2.

[2] أ. د. هدى حامد قشقوش، الحماية الجنائية للتوقيع الإلكتروني، بحث مقدم إلى مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، المجلد الثاني، كلية الشريعة والقانون وغرفة صناعة دبي، 1-12 مايو 2003، ص578.

[3] المرجع نفسه، ص ص 580-581.

عليها بسهولة ويسر، بشكل يظهر إرادته الصريحة في الرضا بالعقد،[1] ويعتبر التوقيع أهم عنصر في المحرر أو الورقة العرفية.[2]

ولا يتطلب القانون لصحة الورقة العرفية وإضفاء الحجية عليها في مواجهة صاحبها إلا إمضاءه عليها، ولا يجوز له التحلل من نسبة الورقة إليه إلا بالادعاء بتزويرها.[3] وفي القانون الفرنسي نجد أن التوقيع يجب أن يتخذ شكلا واحدا، وهو الإمضاء الشخصي، ويجب أن يكون مكتوبا، ولا يجوز أن يأتي في صورة أخرى.[4] ولقد سلك المشرع الجزائري مسلك المشرع الفرنسي، حيث قصر التوقيع على الإمضاء،[5]كما تنص على ذلك م327 ق م.

وللتوقيع عدة شروط يجب توافرها منها أن يكون مطابقا، أي أن يتم وفقا للطريقة التي درج الشخص على استخدامها للتعبير عن موافقته على محرر معين، حيث يجب أن يكون التوقيع دالا على شخصية صاحبه ومميزا لهويته، وتعبيرا عن رضائه الالتزام بمضمون المحرر،[6] كما يجب أن يكون التوقيع دائما، بمعنى أن يتم بوسيلة تترك أثرا متميزا لا يزول، ويجب أن يكون مقروءا ومرئيا خاصة في حالة التوقيع بالإمضاء، رغم أن بعض الأحكام القضائية أقرت التوقيع غير المقروء.[7] ويجب أن يكون التوقيع مباشرا أي أن يتولى الشخص بنفسه وضع التوقيع، وأن يكون مضمنا في المحرر ذاته، والغالب أن يوضع في نهاية الكتابة التي يتضمنها المحرر،[8] ويستوي أن يتم التوقيع باستخدام الاسم واللقب أو مختصرا، أو بالحروف الأولى من الاسم وباللقب كاملا.[9]

مع التطور المذهل الذي أحدثته الانترنت والتجارة الإلكترونية على وجه الخصوص، والخصائص التي تتميز بها هذه التجارة، خاصة الصفقات الضخمة التي تتم عن بعد، كان لزاما إيجاد طريقة أخرى تتلاءم مع طبيعة التجارة الإلكترونية، يتم بواسطتها تحديد هوية صاحبها والتعبير عن

---

[1] ثروت عبد الحميد، التوقيع الإلكتروني، دار الجامعة الجديدة، الأزاريطة، الإسكندرية، مصر2007، ص19.

[2] مناني فراح، أدلة الإثبات الحديثة في القانون، دار الهدى عين مليلة، الجزائر 2008، ص88.

[3] ثروت عبد الحميد، المرجع السابق، ص21.

[4] المرجع نفسه، ص23.

[5] بودالي محمد، التوقيع الإلكتروني، مجلة المدرسة الوطنية للإدارة، المجلد 13، العدد26، 2003، ص52.

[6] المرجع نفسه، ص53، يراجع أيضا: ثروت عبد الحميد، المرجع السابق، ص24.

[7] ثروت عبد الحميد، المرجع السابق، ص25.

[8] ثروت عبد الحميد، المرجع السابق، ص28.

[9] بودالي محمد، المرجع السابق، ص53.

إرادته، فظهر التوقيع الإلكتروني، ولكن المشكلة التي يطرحها هو أن الأشخاص لا يرتبطون بعلاقة قانونية مسبقة، ولا يتم بينهم اتفاقات مباشرة تحسم ما قد يثور بينهم من منازعات، ومن هنا نشطت الجهود الدولية والإقليمية لبحث السبل الكفيلة لإعطاء الثقة في التوقيع الإلكتروني.

ولقد تباينت التعريفات التي أعطيت للتوقيع الإلكتروني، إذ انصب اهتمام بعضها على تبيان الوسائل التي يتم بها، وبعضها الآخر اهتم بالأدوار والوظائف التي يضطلع بها، ومن أوائل هذه التعريفات التعريف الوارد في القانون الفيدرالي الأمريكي المتعلق بالتجارة الإلكترونية، الصادر في 2000/06/30 والذي عرف التوقيع الإلكتروني بأنه عبارة عن: "أصوات أو إشارات أو رموز، أو أي إجراء آخر يتصل منطقيا بنظام معالجة المعلومات إلكترونيا، ويقترن بتعاقد أو مستند أو محرر، ويستخدمه الشخص قاصدا التوقيع على المحرر".[1] أما المشرع الأردني فقد عرفه في م2 من قانون المعاملات رقم 85 لسنة 2001 بأنه: "مجموعة من البيانات تتخذ هيئة حروف أو أرقام أو إشارات أو غيرها، وتكون مدرجة بشكل إلكتروني أو رقمي أو ضوئي أو أية وسيلة أخرى مماثلة في رسالة معلومات أو مضافة عليها أو مرتبطة بها، ولها طابع يسمح بتحديد هوية الشخص الذي وقع عليها، وتميزه عن غيره من أجل توقيعه، وبغرض الموافقة على مضمونه". وبذلك يكون المشرع الأردني قد وضع تعريفا واسعا بغرض استيعاب كل الطرق التقنية الموجودة أو التي قد توجد مستقبلا، والتي يتم بها توقيع المحرر الإلكتروني.[2]

كما يلاحظ من خلال تعريف المشرع الأردني أن التوقيع الإلكتروني عبارة عن وسيلة حديثة لتحديد هوية صاحب التوقيع، ورضائه بالتصرف القانوني الموقع عليه، وهو يقوم بوظائف التوقيع التقليدي ذاتها، بيد أنه ينشأ عبر وسيط إلكتروني استجابة لنوعية المعاملات التي تتم إلكترونيا.[3]

كما عرفت المادة الأولى من القانون المصري رقم 115 لسنة 2004 التوقيع الإلكتروني بأنه "ما يوضع على محرر إلكتروني، ويتخذ شكل حروف أو أرقام أو رموز أو إشارات أو غيرها،

---

[1] المرجع نفسه، ص54.

[2] يوسف زروق، حجية وسائل الإثبات الحديثة، أطروحة دكتوراه في القانون الخاص،جامعة أبي بكر بلقايد، تلمسان 2013/2012، ص222.

[3] عبد الله أحمد عبد الله غرايبة، حجية التوقيع الإلكتروني في التشريع المعاصر، دار الراية للنشر والتوزيع، عمان، الأردن 2008، ص45.

ويكون له طابع متفرد، يسمح بتحديد شخص صاحب التوقيع ويميزه عن غيره"، وعرفت المادة ذاتها المحرر الإلكتروني.[1]

نصت م18 من القانون نفسه على تمتع التوقيع الإلكتروني والكتابة الإلكترونية والمحرر الإلكتروني بالحجية في الإثبات إذا توافرت فيها الشروط التالية:

- ارتباط التوقيع الإلكتروني بالموقع وحده دون غيره.
- سيطرة الموقع وحده دون غيره على الوسيط الإلكتروني.
- إمكانية كشف أي تعديل أو تبديل في بيانات المحرر الإلكتروني أو التوقيع الإلكتروني.

وبالنسبة للقانون التونسي رقم 83 لسنة 2000، المتعلق بالمبادلات والتجارة الإلكترونية، فلم يتضمن تعريفا للتوقيع الإلكتروني، واكتفى في نص م2 من القانون بالتطرق إلى كيفية إنشائه عن طريق التشفير أو المعدات الشخصية المعدة خصيصا لإنشاء التوقيع الإلكتروني.[2]

وقد حثت م1/5-2 من التوجيه الأوربي المتعلق بالتوقيع الإلكتروني الصادر في 1999/12/13 دول أعضاء الاتحاد الأوربي على التأثير القانوني للتوقيع الإلكتروني وقبوله كحجة في الإثبات القانوني، وأنه لا يجوز رفضه لأحد الأسباب التالية:

- أن يكون التوقيع قد قدم في شكل إلكتروني.
- لأنه لم يوضع على شهادة معتمدة.
- لأنه لم يوضع على شهادة معتمدة ومسلمة من أحد مقدمي خدمات التصديق المعتمدين للتصديق على الشهادات.
- لأنه لم ينشأ بنص يأمر بإنشاء هذا التوقيع.

يرى البعض بأن م2/5 لم تستخدم مصطلح التوقيع الإلكتروني المقدم "signature électronique avancée"، وبناء عليه يجوز تطبيق نص هذه المادة على التوقيع الإلكتروني البسيط قبل اعتماده من قبل مقدمي خدمات التصديق المعتمدين لدى الدولة، أي أن هذا التوقيع

[1] سبقت الإشارة في موضع سابق إلى تعريف القانون المصري للمحرر الإلكتروني والذي كان كالآتي: "هو رسالة بيانات تتضمن معلومات تنشأ أو تدمج أو تخزن أو ترسل أو تستقبل كليا أو جزئيا بوسيلة إلكترونية أو رقمية أو ضوئية أو بأية وسيلة أخرى مشابهة".

[2] يوسف زروق، المرجع السابق، ص223.

الإلكتروني البسيط يتوجب قبوله كدليل للإثبات، وعند حدوث ازدواجية بين توقيعين إلكترونيين أحدهما بسيط والآخر مقدم، تكون الأولوية للتوقيع المقدم لتمتعه بعناصر أمان.[1]

كما أن قانون الأونسترال النموذجي بشأن التوقيعات الإلكترونية الصادر سنة 2001، أورد تعريفا للتوقيع الإلكتروني في المادة الثانية منه.

وفي إطار الموجة العالمية الدافعة لمزيد من التعاملات الإلكترونية أصدر المشرع الفرنسي قانون 13 مارس 2000، المتعلق بالدليل والتوقيع الإلكترونيين.[2]

من خلال تعديل م4/1316 نص المشرع الفرنسي في القانون المدني على التوقيع الإلكتروني بأنه يتمثل في استعمال وسيلة آمنة تكفل تحديد هوية الشخص، وتضمن صلته بالتصرف الملحق به، وتفترض موثوقية تلك الوسيلة إلى غاية حدوث العكس، وصدر بعد ذلك مرسوم عن مجلس الدولة الفرنسي رقم 272 لسنة 2001 الخاص بتطبيق نص م4/1316 ق م ف، وميز هذا المرسوم في التعريف بين نوعين من التوقيعات الإلكترونية: النوع الأول هو التوقيع الإلكتروني البسيط، ويتمثل في مجموعة من البيانات تنشأ عن استخدام وسيلة آمنة لتحديد الشخص، وتضمن صلته بالتصرف الذي وقع عليه، أما النوع الثاني فهو التوقيع الإلكتروني المؤمَّن، وهو ذلك التوقيع الذي يستوفي المتطلبات التالية:

- أن يكون خاصا بالموقع نفسه.
- أن ينشأ بوسيلة تكون تحت سيطرة الموقّع وحده.
- أن يضمن اكتشاف أي تعديل لاحق يحدث في البيانات.

أما بخصوص المشرع الجزائري فقد نص على التوقيع الإلكتروني سنة 2005، بعد تعديل القانون المدني بالقانون 05-02[3] من خلال نص م327 ق م، ورغم اعتراف المشرع الجزائري بالتوقيع الإلكتروني إلا أنه لم يعرفه في القانون المدني، إذ نص على الاعتداد بالتوقيع الإلكتروني وفق الشروط المذكورة في م و323 مكرر1 ق م، واستدرك الأمر من خلال نص م3 من المرسوم التنفيذي رقم 07-

[1] د.سعيد السيد قنديل، التوقيع الالكتروني، ط2، دار الجامعة الجديدة للنشر، الأزاريطة، الإسكندرية، مصر، 2006 ص 54.

[2] Aboudramane Ouattara, la preuve électronique, étude de droit comparé Afrique Europe Canada, presses universitaires d'aix Marseille, 2011, p183.

[3] المؤرخ في 20 يونيو 2005، ج ر 44، ص24.

162 المؤرخ في 30 مايو 2007، وعرف التوقيع الإلكتروني على النحو التالي: "التوقيع الإلكتروني معطى ينجم عن استخدام أسلوب عمل يستجيب للشروط المحددة في المادتين 323 مكرر و323 مكرر1 من الأمر 75-58..."

وتطرقت المادة ذاتها إلى التوقيع الإلكتروني المؤمن، وذكرت بأنه توقيع إلكتروني يفي بالمتطلبات التالية:

- يكون خاصا بالموقع.
- يتم إنشاؤه بوسائل يمكن أن يحتفظ بها الموقع تحت مراقبته الحصرية.
- يضمن مع الفعل المرتبط به، صلة بحيث يكون كل تعديل لاحق للفعل قابلا للكشف عنه.[1]

مواكبة منه للتطورات الجارية على الساحة العالمية في المجال الإلكتروني، سواء ما تعلق منها بالتجارة الإلكترونية أو الحكومة الإلكترونية، أصدر المشرع الجزائري القانون رقم 15-03 والقانون رقم 15-04 المؤرخان في أول فبراير 2015،[2] ويتعلقان على التوالي بعصرنة العدالة، وتحديد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، والملفت للانتباه أن المشرع الجزائري جاء في م07 من القانون رقم 15-04 سالف الذكر بمصطلح جديد هو التوقيع الإلكتروني الموصوف، وعرفه بأنه التوقيع الإلكتروني الذي تتوافر فيه المتطلبات التالية:

- أن ينشأ على أساس شهادة تصديق إلكتروني موصوفة،
- أن يرتبط بالموقع دون سواه،
- أن يمكن من تحديد هوية الموقع،
- أن يكون مصمما بواسطة آلية مؤمنة خاصة بإنشاء التوقيع الإلكتروني،
- أن يكون منشأ بواسطة وسائل تكون تحت التحكم الحَصري للموقّع،
- أن يمون مرتبطا بالبيانات الخاصة به، بحيث يمكن الكشف عن التغييرات اللاحقة بهذه البيانات.

[1] تراجع: م3 من المرسوم التنفيذي رقم 07-162 المؤرخ في 30 مايو 2007، المعدل والمتمم للمرسوم التنفيذي رقم 01-123 المؤرخ في 09 مايو 2001، والمتعلق بنظام الاستغلال المطبق على كل نوع من الشبكات بما فيها اللاسلكية الكهربائية وعلى مختلف خدمات المواصلات السلكية واللاسلكية. ج ر 37 الصادرة في 07 يونيو 2007، ص13.

[2] ج ر 06، الصادرة في 10 فبراير 2015، ص4-16.

الملاحظ بالنسبة للتوقيع الموصوف أنه يضم متطلبات التوقيع المؤمن ومتطلبات أخرى، وقد اعتبرت م08 من القانون 15-04 التوقيع الإلكتروني الموصوف وحده مماثلا للتوقيع المكتوب، سواء كان لشخص طبيعي أو معنوي، غير أن هذا لا يعني تجريد التوقيع الإلكتروني من فعاليته القانونية أو رفضه كدليل أمام القضاء بسبب شكله الإلكتروني، أو أنه لا يعتمد على شهادة تصديق إلكتروني موصوفة، أو أنه لم يتم إنشاؤه بواسطة آلية مؤمنة لإنشاء التوقيع الإلكتروني (م09 من القانون 15-04).

عرفت م1/2 من القانون 15-04 التوقيع الإلكتروني بأنه: "بيانات في شكل إلكتروني، مرفقة أو مرتبطة منطقيا ببيانات إلكترونية أخرى، تستعمل كوسيلة توثيق".

يلاحظ على هذه التعريفات أنها جاءت متسقة مع مبدأين مهمين من مبادئ التجارة الإلكترونية وهما:

- أن تعريف التوقيع الإلكتروني جاء متسقا مع مبدأ الحياد إزاء التكنولوجيا، وهو مبدأ يقوم على حرية السوق التنافسية، بمعنى أنه غير متحيز إلى طريقة تكنولوجية معينة دون أخرى، ما دامت أن كل واحدة منها بإمكانها القيام بدور التوقيع التقليدي.
- استقلالية الأطراف، بمعنى أن تكون أطراف التجارة الإلكترونية قادرة بنفسها على تحديد القواعد والمعايير التي تطبق على علاقاتها التجارية.[1]

عرف بعض الفقه التوقيع الإلكتروني بأنه مجموعة من الإجراءات والوسائل التي يتبع استخدامها عن طريق الرموز أو الأرقام إخراج رسالة إلكترونية، تتضمن علامة مميزة لصاحب الرسالة المنقولة إلكترونيا، يجري تشفيرها باستخدام زوج من المفاتيح، واحد معلن، والآخر خاص بصاحب الرسالة.[2]

يجمع الفقه الراجح بين الإشادة بوظائف التوقيع الإلكتروني ووسائله وأدواته، مع الإشارة إلى الجهات المختصة باعتماده، وعلى هذا الأساس يعرف التوقيع الإلكتروني بأنه عبارة عن: "إشارات أو رموز أو حروف مرخص بها من الجهة المختصة باعتماد التوقيع، ومرتبطة ارتباطا وثيقا

[1] عبد الله أحمد عبد الله، المرجع السابق، ص46.

[2] د. عيسى غسان ربضي، القواعد الخاصة بالتوقيع الإلكتروني، دار الثقافة للنشر والتوزيع، عمان، الأردن 2009، ص55.

بالتصرف القانوني، بحيث تسمح بتمييز شخص صاحبها، وتحديد هويته، وتكشف دون غموض عن رضائه بهذا التصرف القانوني".[1]

بناء على ماسبق، نلحظ أن التوقيع الإلكتروني له وظيفة التوقيع التقليدي نفسها، فكلاهما يستهدف تحديد هوية الموقع، وانصراف الإرادة لإبرام التصرف القانوني محل التوقيع، كما أنهما يتفقان أيضا من حيث ضرورة اتصال التوقيع بالمحرر اتصالا وثيقا لا يقبل الانفصال، فضلا عن ذلك فإن كلا منهما له حجية في الإثبات، إلا أن التوقيع الإلكتروني والتوقيع التقليدي يختلفان في بعض الأمور منها أن بعض التشريعات تقصر صور التوقيع في الشكل الكتابي على الإمضاء، ويضاف إليها بصمة الختم وبصمة الأصابع بالنسبة لتشريعات أخرى، أما التشريعات المتعلقة بالتوقيع الإلكتروني فقد أجازت أن يكون في أي قالب: أحرف أو أرقام أو رموز أو إشارات بل حتى أصوات، طالما أن لها طابعا منفردا يحدد هوية صاحبه، ويؤكد إرادته في إنفاذ التصرف؛ كما يختلف التوقيع الإلكتروني من حيث الشكل عن التوقيع العادي، بحيث أن هذا الأخير يفرغ في محرر ورقي، أما التوقيع الإلكتروني فيتم من خلال وسيط إلكتروني تتعدد صوره، وفي بيئة إلكترونية؛ كما يختلف التوقيعان في عنصر الثقة والأمان، بحيث أن التوقيع الإلكتروني أكثر ثقة وأمانا بفضل وجود سلطة مختصة يجوز للمتعاقد الآخر الرجوع إليها قبل توقيعه؛ كما يختلف التوقيع الإلكتروني عن التوقيع العادي من حيث نطاق الحماية الجزائية، بحيث يتصور انطباق كافة النصوص المتعلقة بحماية التوقيع التقليدي كجرائم اختلاس التوقيع، والإكراه بالتوقيع على سند، وتزوير التوقيع، بالإضافة إلى جرائم أخرى متعلقة بالتوقيع الإلكتروني وحده كالدخول غير المشروع على قاعدة بيانات تتعلق بالتوقيع الإلكتروني، وكذا صنع وحيازة برنامج لإعداد توقيع إلكتروني، وفض مفاتيح التشفير.[2]

2- صور التوقيع الإلكتروني.

يستعمل التوقيع الرقمي في التعاملات البنكية وغيرها، وأوضح مثال عليه بطاقة الائتمان التي تحتوي على "رقم سري" لا يعرفه سوى العميل الذي يدخل البطاقة في جهاز السحب الآلي،

[1] بودالي محمد، المرجع السابق، ص56.

[2] أيمن رمضان، المرجع السابق، ص ص34-36.

حين يطلب الاستعلام عن حسابه أو صرف جزء من رصيده، وهي تعمل بنظامي "Off – Line" ثم نظام ."ON – Line".[1]

وفي حالة نظام "Off – Line" يتم تسجيل العملية على شريط مغناطيسي، ولا يتغير موقف العميل المالي، في حسابه إلا في آخر اليوم، بعد انتهاء ساعات العمل.

أما في حالة نظام "On – Line" ففيه يقيد موقف العميل ويتم تحديثه فور إجراء العملية وهو الغالب في التعامل في نظام البطاقات الذكية التي تحتفظ بداخلها بذاكرة تسجل كل عمليات العميل، كما يستخدم التوقيع الإلكتروني الرقمي في المراسلات الإلكترونية التي تتم بين التجار الموردين أو بين الشركات فيما بينها[2].

وقد ظهرت أشكال أو صور متعددة للتوقيع الإلكتروني كالتوقيع الرقمي والتوقيع البيومتري والتوقيع بالقلم الالكتروني.

أ- التوقيع الرقمي:

هو عبارة عن مجموعة من الأرقام التي ترتبط برسالة بيانات فتحولها من رسالة مقروءة إلى رسالة غير مقروءة (مشفرة)، لا يمكن فك تشفيرها إلا من قبل الشخص الذي لديه المفتاح الذي يفك هذا التشفير، فالمعاملات الإلكترونية تتم عن طريق تبادل رسائل البيانات بين الأطراف بشكل مشفر يضمن السرية والخصوصية، ولكي تتم عملية التشفير لا بد من وجود مفتاحين: المفتاح العام والمفتاح الخاص، حيث يستخدم المرسل المفتاح الخاص لكي يوقع على رسالة البيانات التي يريد إرسالها، وهي مجموعة من الأرقام تقوم على معادلة رياضية من شأنها تحويل المعلومات الموجودة في رسالة البيانات إلى رموز مشفرة لا يمكن لأي شخص قراءتها ما لم يفك التشفير، وذلك عن طريق المفتاح العام الذي يكون متاحاً للآخرين،[3] ذلك أن الموقّع المرسل يعلن عن المفتاح العام ليتمكن الآخرون من فك تشفير الرسائل التي يرسلها إليهم.

---

[1] عبد الفتاح بيومي حجازي، التوقيع الإلكتروني في النظم القانونية المقارنة، دار الفكر الجامعي، الإسكندرية، مصر 2005، ص23.

[2] المرجع نفسه، ص24.

[3] مليكة حنان، النظام القانوني للتوقيع الإلكتروني في ضوء قانون التوقيع الإلكتروني السوري رقم 4 الصادر في 2009/02/25، مجلة جامعة دمشق للعلوم القانونية والاقتصادية، المجلد 26، العدد 2، 2010، ص562.

وقد عرف المشرع الجزائري في م8/2 من القانون 15-04 سالف الذكر، مفتاح التشفير الخاص بأنه: "عبارة عن سلسلة من الأعداد يحوزها حصريا الموقّع فقط، وتستخدم لإنشاء التوقيع الإلكتروني، ويرتبط هذا المفتاح بمفتاح تشفير عمومي"، كما عرف في م 9/2 من القانون السابق مفتاح التشفير العمومي بأنه: "عبارة عن سلسلة من الأعداد تكون موضوعة في متناول الجمهور بهدف تمكينهم من التحقق من الإمضاء الإلكتروني، وتدرج في شهادة التصديق الإلكتروني".

يؤمن التوقيع الرقمي درجة عالية من الموثوقية والمصداقية، فهو يقوم على أرقام سرية تعالج بطريقة رياضية تجعل رسائل البيانات المتبادلة مشفرة غير مقروءة بشكل يضمن سرية المعلومات، فضلاً عن وجود هيئة مختصة بتوثيق التوقيعات الإلكترونية وتصديقها.

إن التوقيع الإلكتروني الرقمي له نفس قوة التوقيع التقليدي إن لم نقل أنه ذا قوة أفضل، ولما له من مزايا:

- التوقيع الرقمي دليل على الحقيقة، وبدرجة أكثر من التوقيع التقليدي،و"مفتاح إعلان الحرب النووية" لأكبر دليل على ذلك، فرئيس الدولة هو الوحيد الذي يملك التوقيع ويعلم ذلك الرقم، ومن ثم الوحيد الذي يملك إشارة الحرب، ولخطورة نتائج التوقيع فقد حصرت في رئيس الدولة وهي رقم، وليس توقيعا ضمانا للسرية.

- التوقيع الرقمي يسمح بإبرام الصفقات عن بعد دون حضور المتعاقدين جسدا، وبالتالي يساعد على تنمية وضمان التجارة الإلكترونية. - التوقيع الرقمي وسيلة مأمونة بتحديد هوية الشخص الذي قام بالتوقيع، حيث أنه بعد اتباع إجراءات معينة يمكن التأكد عن طريق الحاسب الآلي أن من قام بالتوقيع هو صاحب التوقيع.[1]

كما أن للتوقيع الرقمي إيجابيات، فإن له سلبيات أيضا، منها:[2]

[1] بيومي حجازي، المرجع السابق، ص26.

[2] المرجع نفسه، ص27-29.

– احتمال تعرضه للسرقة أو الضياع كما أن التوقيع الالكتروني عرضة للتزوير والتقليد، ولتجنب ذلك فعلى العميل الاحتفاظ بسرية الرقم وإلا فيتحمل المسؤولية طالما لم يتخذ إجراءات الحيطة المتفق عليها.

– كما أنه يمكن تقليد الشريط الممغنط الموجود على البطاقة الائتمانية، وهذا أمر يمكن حصوله، لكن استعمال البطاقة لا يتم دون الرقم السري، هذا الأخير لا يعلمه سوى العميل والحاسب الآلي الذي أخرجه لذا فتقليد البطاقة لا يجدي ما لم يعرف الشخص الرقم السري.

– يشاع كذلك أن التوقيع الرقمي لا يعبر عن شخصية صاحبه مثل التوقيع التقليدي بالكتابة، لكن ذلك مردود عليه، حيث أن التوقيع الإلكتروني لا يصدر عن الحاسب، إنما عن صاحب التوقيع فالحاسب الآلي ما هو إلا وسيلة في أداء هذا التوقيع، مثل القلم الذي يعتبر وسيلة للتوقيع التقليدي، لذا على العميل المحافظة على رقمه السري للبطاقة والإبقاء عليه في طي الكتمان لأنه بمثابة مفتاح خزانة النقود، ولذا يسأل صاحب الرقم السري عن خطئه أو إهماله في الحفاظ على رقمه السري، ويتحمل المسؤولية المدنية عن العمليات المنفذة قبل إخطاره بواقعة السرقة.

هناك طرق لتشفير التوقيع الإلكتروني الرقمي، ويعد التشفير إجراء يؤدي إلى توفير الثقة في المعاملات الإلكترونية، وسواء أكان التشفير تناظريا "Symétrique" أم تم بطريقة المفتاح العام، فهدفه يصب في شيء واحد، وهو ضمان الأمان في المعاملات الإلكترونية؛ ولضمان الأمان في عملية التشفير الخاصة بالتوقيع الإلكتروني فقد أوجدت القوانين المقارنة طرفا ثالثا في عمليات التجارة الإلكترونية، يكون محل ثقة الأفراد، ويتمثل في هيئة مختصة يكون لها سلطة إشهار وتوثيق التوقيع الإلكتروني، وهذا الشخص الثالث طرف محايد اعترفت به بعض القوانين المقارنة منها: التوجه الأوربي رقم 1999/93في شأن إطار التوقيع الإلكتروني، وكذلك مشروع قانون التجارة الإلكترونية المصري، وقانون التجارة الإلكترونية التونسي والأمريكي،[1]والقانون الجزائري رقم 15-04 سالف الذكر حيث نصت م11/2 على الطرف الثالث الموثوق، وهو شخص معنوي يقوم بمنح شهادات تصديق إلكتروني موصوفة، وقد يقدم خدمات أخرى متعلقة بالتصديق الإلكتروني لفائدة المتدخلين في الفرع الحكومي.

[1] سعيد السيد قنديل، المرجع السابق، ص52. ويراجع أيضا: بيومي حجازي، المرجع السابق، ص32.

ب- التوقيع البيومتري:

يقوم التوقيع البيومتري على خصائص بيولوجية ترتبط بجسم الإنسان كبصمة أصبعه أو صوته أو الشبكية في عينه، وتختص به دون غيره؛ ذلك أن هذه الصفات تختلف من شخص إلى آخر مما يجعل هذا التوقيع متمتعا بدرجة عالية من درجات الموثوقية التي تدفع المتعاملين إلكترونيا إلى اعتماده أساسا في تعاملاتهم.

ويتجسد هذا التوقيع بأخذ عينة من إحدى الخصائص البيولوجية الخاصة بالموقع دون غيره، ثم تخزن عن طريق التشفير إلكترونياً ليتم مطابقتها بتلك المستخدمة في معاملات إلكترونية.

يحتاج التوقيع البيومتري إلى توثيقه من جهة مختصة معتمدة بشكل رسمي تقوم بتوثيق التوقيع وتصديقه، وتربط بينه وبين الموقع وذلك لزيادة الموثوقية وتحقيق الأمان في التعامل الإلكتروني، وحماية المتعاملين من التقنيات الاحتيالية المتبعة لفك رموز التشفير.

يتشابه كل من التوقيع الرقمي والتوقيع البيومتري، في أن كلا منهما يقوم على التشفير ومعالجة البيانات المتبادلة إلكترونيا، بوجود سلطة التوثيق التي تعمل على توثيق التوقيع الإلكتروني وتصديقه.[1]

ج- التوقيع بالقلم الالكتروني.

يتم هذا التوقيع باستخدام القلم الالكتروني الذي يمكن مستخدمه من التوقيع على شاشة الكمبيوتر بشكل مباشر عن طريق برنامج حاسوبي حيث يحتفظ في البداية بالتوقيع الشخصي للمستخدم ويخزن بياناته الخاصة، فإذا ما وقع المستخدم على إحدى الوثائق الإلكترونية فإن هذا البرنامج الإلكتروني يتحقق من صحة التوقيع فيطابق بين هذا التوقيع والتوقيع المخزن لديه.

ويتجسد التوقيع بالقلم الالكتروني بحركة يد الموقع وهو يستخدم القلم الالكتروني لتكوين التوقيع الإلكتروني الذي يتم تشفيره الكترونيا، ثم يتم استرجاعه للمقارنة بينه وبين التوقيع الذي يجريه المستخدم بالقلم الالكتروني عند قيامه بأية معاملة الكترونية.

[1] مليكة حنان، المرجع السابق، ص563.

يؤكد الموقع أنه مسؤول عن الكتابة التي وقع عليها مهما كان شكل التوقيع لأن أي رمز صادر عن الموقع يعبر فيه عن إرادته لتبني ما وقع عليه فهو توقيع مقبول.

إن التطور التقني المستمر يفرض أشكالاً جديدة متطورة للتوقيع الإلكتروني على أن تحقق الهدف الأساسي منه، المتمثل في تحديد هوية الموقع والتعبير عن إرادته في الالتزام بما وقع عليه.[1]

ثانيا: صور الاعتداءات الواقعة على التوقيع الالكتروني.

جرائم الاعتداء على التوقيع الالكتروني من الجرائم التي تقع على مضمون التجارة الالكترونية نفسها، لأن عقود التجارة الالكترونية يستلزم لصحتها تمام توقيع الطرفين، الذي يتم إلكترونيا.[2]

وتتنوع جرائم الاعتداء على التوقيع الالكتروني، ومن أخطر هذه الجرائم: الدخول بطريق الغش على قاعدة بيانات تتعلق بالتوقيع الالكتروني، صنع أو حيازة برنامج لإعداد توقيع إلكتروني، تزوير وتقليد المحررات الإلكترونية والتوقيع الإلكتروني... ولقد تطرقت تشريعات مقارنة لمجموعة من صور هذه الجرائم، كما تطرق المشرع الجزائري في القانونين 15-03 و15-04 خاصة إلى بعض هذه الجرائم.

1- الدخول بطريق الغش على قاعدة بيانات تتعلق بالتوقيع الإلكتروني:

نصت على هذه الجريمة م26 من مشروع التجارة الإلكترونية المصري، يقع الركن المادي لهذه الجريمة على نظام معلومات أو قاعدة بيانات تتعلق بالتوقيع الالكتروني نفسه، وقد نصت م26 من المشروع على: "مع عدم الإخلال بأية عقوبة أشد وردت في قانون آخر، يعاقب بالحبس وبغرامة لا تقل عن ثلاثة آلاف جنيه أو بإحدى هاتين العقوبتين، كل من دخل بطريق الغش أو التدليس على نظام معلومات أو قاعدة بيانات تتعلق بالتوقيعات الإلكترونية، ويعاقب بالعقوبة نفسها من اتصل أو أبقى الاتصال بنظام المعلومات أو قاعدة البيانات بصورة غير مشروعة".

---

[1] مليكة حنان، المرجع السابق، ص564.

[2] بيومي حجازي، الحماية الجنائية...الكتاب الثاني، المرجع السابق، ص294.

لم يشترط المشرع المصري في م26 تحقق نتيجة معينة على إثر الدخول، فكل ما اشترطه أن يتم هذا الدخول عن طريق الغش أو التدليس، لذلك تصنف هذه الجريمة من ضمن جرائم الخطر.

ويعتبر من قبيل الغش أو التدليس المعلوماتي أن يتم الولوج إلى قاعدة البيانات أو النظام المعلوماتي دون إذن قضائي، أو من قبل أشخاص لا يجوز لهم الاطلاع على هذا النظام أو قاعدة البيانات المتعلقين بالتوقيع الالكتروني.

أما الصورة الأخرى للركن المادي لهذه الجريمة فهي قيام الجاني بالاتصال بنظام المعلومات أو قاعدة البيانات أو إبقاء الاتصال به بطريقة غير مشروعة، ومعنى ذلك أن الجاني ليس له الحق بالاتصال بهذين النظامين المتعلقين بالتوقيع الالكتروني فاتصل بهما، أو أن للجاني حق الاتصال خلال فترة زمنية محددة، أو في أوقات محددة، وأبقى الاتصال خارج الفترة المسموح له الاتصال فيها.

هذه الجريمة عمدية صورة الركن المعنوي فيها هو القصد الجنائي العام بعنصريه العلم والإرادة: علم الجاني بحقيقة سلوكه الإجرامي وأن ذلك محظور عليه قانونا، وانصراف إرادته رغم ذلك إلى السلوك الإجرامي.[1] وهذه الجريمة شبيهة بجريمة الدخول أو البقاء غير المشروعين إلى مواقع التجارة الإلكترونية، والتي تم دراستها في الباب الأول، غير أنها تتعلق فقط بالتوقيع الإلكتروني، وعليه يجوز القول أنها تطبيق من تطبيقات جريمة الدخول أو البقاء على المواقع الإلكترونية للتجارة الإلكترونية، وعليه نرى بأن م394 مكرر ق ع والتي تنص على: "يعاقب بالحبس من ثلاثة أشهر إلى سنة وبغرامة من 50.000 د ج إلى 100.000 د ج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك" يجوز تطبيقها بخصوص الدخول أو البقاء غير المشروعين أو الشروع في ذلك في كل أو جزء من قاعدة بيانات أو نظام معلومات للتوقيع الإلكتروني.[2] والملاحظ أن المشرع الجزائري قد عاقب على الشروع في هذه الجريمة على خلاف المشرع المصري.

[1] بيومي حجازي، المرجع السابق، ص298.

[2] أيمن رمضان، المرجع السابق، ص123 وما بعدها.

2- صنع أو حيازة برنامج لإعداد توقيع إلكتروني.

يتمثل الركن المادي لهذه الجريمة حسب نص م27 من مشروع القانون المصري حول التجارة الالكترونية، في صور عديدة هي صناعة نظام معلوماتي أو برنامج لإعداد توقيع إلكتروني، أو حيازة النظام أو البرنامج المذكورين، أو الحصول على أي منهما بغرض إعداد التوقيع الالكتروني دون موافقة صاحبه.

محل الجريمة هنا هو إعداد توقيع إلكتروني دون موافقة صاحبه، عن طريق نظام معلوماتي أو برنامج.

قد يقوم الجاني في هذه الجريمة بصناعة البرنامج أو النظام المعلوماتي، أي إيجاده من عدم، ويستوي في هذه الحالة أن يكون الجاني شخصا طبيعيا أو معنويا، مرخصا له بالعمل في هذا المجال أو غير مرخص، طالما لا توجد موافقة من ذوي الشأن من أجل استخراج توقيع إلكتروني، ويستوي كذلك الوسيلة الفنية المستعملة، ولكن يجب أن تكون قادرة على صنع توقيع إلكتروني.

إذا توافرت هذه الشروط (صناعة برنامج أو نظام معلوماتي له المقدرة الفنية لعمل توقيع إلكتروني رغما عن إرادة صاحب التوقيع) توافرت عناصر الركن المادي لهذه الجريمة بغض النظر عن تمام استخراج التوقيع من عدمه، ولذلك يمكن القول أن هذه الجريمة من جرائم السلوك المجرد أو جرائم الخطر التي لا تشترط ضرورة حصول نتيجة إجرامية معينة وهي الحصول على توقيع إلكتروني للمجني عليه.[1]

الصورة الثانية لهذه الجريمة هي حيازة برنامج أو نظام معلوماتي لإعداد توقيع إلكتروني دون موافقة صاحبه.

الفرض هنا أن البرنامج أو النظام المعلوماتي الذي في حيازة الجاني هو برنامج حيازته غير مشروعة، لأنه غير مرخص له بهذه الحيازة من الجهة المانحة للتراخيص.

إذا ما توافرت الحيازة غير المشروعة في حق الجاني توافر الركن المادي للجريمة دون حاجة لتمام التوقيع الإلكتروني، فهذه الصورة أيضا من جرائم الخطر.

[1] بيومي حجازي، المرجع السابق، ص300.

أما الصورة الثالثة للركن المادي لهذه الجريمة فهي الحصول على نظام معلوماتي أو برنامج لإعداد توقيع إلكتروني دون موافقة صاحب الشأن.

الفرض في هذه الصورة أن هذا الحصول تم بصورة غير مشروعة، أي أن الجاني ليس له الحق في الحصول على النظام أو البرنامج، فليس من المرخص لهم بذلك، ولا تهم طريقة الحصول على البرنامج، سواء تم الحصول بالسرقة أو الاستئجار أو الشراء أو العارية من قبل أحد المرخص لهم بامتلاك البرنامج.

ويجب توافر الركن المعنوي أيضا لقيام هذه الجريمة في مختلف صورها، ويتمثل في القصد الجنائي العام بعنصريه، العلم والإرادة.[1]

3- تزوير وتقليد المحررات الإلكترونية والتوقيع الإلكتروني.

حسب نص م28 من مشروع القانون المصري المتعلق بالتجارة الإلكترونية فإن الركن المادي لهذه الجريمة له صور عديدة تتمثل في تزوير أو تقليد محرر إلكتروني أو شهادة اعتماد توقيع إلكتروني، أو استعمال محرر أو توقيع إلكتروني مزور أو شهادة مزورة باعتماد توقيع إلكتروني شرط أن يكون الفاعل عالما بذلك.

ويتمثل الركن المادي لهذه الجريمة في صوره المتعددة في فعل التزوير أو التقليد الإلكتروني، واستعمال هذه المحررات الإلكترونية المزورة بما فيها التوقيع الإلكتروني المزور.

في نظام جرائم الحاسب الآلي، فإن التزوير الإلكتروني أو المعلوماتي يعني "أي تغيير للحقيقة يرد على مخرجات الحاسب الآلي، سواء تمثلت في مخرجات ورقية مكتوبة، أو كانت مرسومة عن طريق الراسم، ويستوي في المحرر المعلوماتي أن يكون مدونا بالعربية أو بأية لغة أخرى، كذلك قد يتم في مخرجات غير ورقية شريطة أن تكون محفوظة على دعامة، كبرنامج منسوخ على أسطوانة، وشرط أن يكون المحرر المعلوماتي ذا أثر في إثبات حق أو أثر قانوني معين".[2]

---

[1] المرجع نفسه، ص303.

[2] بيومي حجازي، المرجع السابق، ص306.

رأينا فيما سبق، أن المشرع الفرنسي قد استوعب ضمن التزوير التقليدي حالة الغش المعلوماتي الواقع على وثيقة معلوماتية، وذلك بالنص على لفظ "أي سند أو دعامة، وبأي وسيلة"، فلم يحدد المشرع طريقة معينة للتزوير[1].

وبناء عليه، فإن التزوير المعلوماتي يرد على وثائق معلوماتية، وهي الوثائق التي تكون ناشئة عن جهاز إلكتروني أو كهرومغناطيسي أو طبع ممغنط، وإن كان جانب من الفقه يرى عدم الخلط بين الوثائق المبرمجة والوثائق المعلوماتية، إذ أن الوثيقة المعلوماتية وثيقة لم تبرمج بعد.

وقد عرفت الوثيقة المعلوماتية بأنها: "كل جسم منفصل أو يمكن فصله عن نظام المعالجة الآلية للمعلومات، وقد سجلت عليه معلومات معينة سواء كان معدا للاستخدام بواسطة نظام المعالجة الآلية للمعلومات أو يكون مشتقا من هذا النوع".[2]

ولا يمكن تعريف الوثيقة المعلوماتية أو المحرر المعلوماتي إلا بالرجوع لما يسمى نظام المعالجة الآلية للمعطيات.

الصورة الأولى للركن المادي في هذه الجريمة هي تزوير أو تقليد محرر إلكتروني، وقد عرف المشرع المصري المحرر الإلكتروني في قانون التوقيع الإلكتروني، وفكرة المحرر الإلكتروني حسب المشرع المصري تنصرف إلى أي معلومة أو بيان يعالج إلكترونيا، ولذلك فإن وقع التزوير بمفهومه السابق على محرر إلكتروني حسب هذا المفهوم تحقق الركن المادي لهذه الجريمة، ويندرج ضمن هذه الحالة المحرر المعلوماتي بمفهومه السابق.كذلك يتحقق التزوير المعلوماتي إن كان موضوع هذا التزوير أو التقليد المعاقب عليه، التوقيعُ الالكتروني.كما أن تزوير أو تقليد شهادات التصديق على التوقيع الالكتروني يعادل في خطورته تزوير أو تقليد التوقيع الالكتروني ذاته.

أما الجريمة الثانية التي عاقب عليها المشرع بالعقوبة ذاتها فهي جريمة استعمال التوقيع الالكتروني المزور أو المقلد، وكذلك المحرر الالكتروني المزور أو المقلد، وكذلك شهادة اعتماد التوقيع الالكتروني المزورة، وذلك فيما زورت أو قلدت لأجله.[1]

---

[1] المرجع نفسه، ص307.

[2] المرجع نفسه، ص307.

هذه الجريمة في صورتيها، سواء التزوير أو استعمال المزور الالكتروني جريمة عمدية، صورة الركن المعنوي فيها هو القصد الجنائي بعنصريه العلم والإرادة، حيث يجب أن يعلم الجاني بوقائع الجريمة وأن ذلك محظور وفقا للقانون، ومع ذلك تتجه إرادته إلى الفعل المجرم ويقبل النتيجة المترتبة عليها (القصد العام) بغية استعمال المحرر الإلكتروني المزور (القصد الخاص). وكذلك في جريمة الاستعمال لا بد أن يعلم الجاني أن المحرر الإلكتروني مزور أو مقلد، ورغم ذلك تنصرف إرادته إلى استعماله فيما أعد له.[2]

4- الاستعمال غير القانوني للعناصر الشخصية المتصلة بإنشاء توقيع إلكتروني تابع للغير.

نصت على هذه الجريمة م17 من القانون 15-03 سالف الذكر: "يعاقب بالحبس من سنة إلى خمس سنوات وبغرامة تتراوح بين 100.000 و500.000 دج كل شخص يستعمل بطريقة غير قانونية العناصر الشخصية المتصلة بإنشاء توقيع إلكتروني يتعلق بتوقيع شخص آخر".[3]

الملاحظ حول هذه الجريمة أنها جنحة، كما يلاحظ أيضا أن المشرع لم يجرم على محاولة ارتكاب هذه الجريمة، وبالتالي لا عقاب على الشروع فيها، كما لم ينص المشرع على مسؤولية الشخص المعنوي، والسؤال المطروح هل يجوز تفسير كلمة "كل شخص" الواردة في المادة على أنها تعني كل شخص طبيعي أو معنوي، وخاصة وأن العبارة بالفرنسية "quiconque" جاءت عامة؟ أم لا مجال للتوسع، إذ كان بإمكان المشرع أن ينص صراحة على مسؤولية الشخص المعنوي لو أراد ذلك، كما فعل في القانون 15-04 الصادر في الجريدة الرسمية ذاتها (م75).

الركن المادي لهذه الجريمة هو استعمال العناصر الشخصية المعدة خصيصا لإنشاء توقيع إلكتروني للغير استعمالا غير قانوني، وهذه العبارة واسعة، وقد أحسن المشرع عند ذكرها، إذ يخرج من

---

[1] بيومي حجازي، المرجع السابق، ص309.

[2] المرجع نفسه، ص310.

[3] جاءت صياغة النص باللغة الفرنسية كالآتي:

Art. 17. . Est puni d'un emprisonnement d'un an (1) à cinq (5) ans et d'une amende de 100.000 DA à 500.000 DA, quiconque utilise de façon illégale les éléments de création de signature personnels relatifs à la signature électronique d'autrui.

دائرة الاستعمال، ذلك الاستعمال المشروع فقط والذي يكون في إطار ما يجيزه القانون حسب القواعد العامة، عدا ذلك يعتبر الاستعمال غير مشروع؛ ولم يتطلب المشرع تحقق نتيجة فبمجرد الاستعمال يقوم الركن المادي لهذه الجريمة، فهذه الجريمة إذن من جرائم السلوك، أو ما يسمى أيضا جرائم الخطر وليست من جرائم الضرر.

أما فيما يخص الركن المعنوي، فيبدو أنها تخضع للقواعد العامة، أي ضرورة توافر القصد العام بعنصريه العلم والإرادة: العلم بأن هذه العناصر تدخل في إطار إنشاء توقيع إلكتروني متصل بتوقيع الغير، وتوجه الإرادة رغم ذلك إلى نية استعمالها، ولا يشترط قصد خاص حسب نص المادة.

5- جريمة الإقرار الكاذب للحصول على شهادة تصديق إلكتروني موصوفة.

نص المشرع الجزائري في القانون رقم 15-04 الخاص بالتوقيع والتصديق الإلكترونيين على عقوبة الحبس من ثلاثة أشهر إلى ثلاث سنوات، والغرامة من 20.000 إلى 200.000 دج أو بإحدى هاتين العقوبتين في حق كل من أدلى بإقرارات كاذبة للحصول على شهادة تصديق إلكتروني موصوفة، فالمشرع الجزائري في هذه المادة يجرم الإقرار الكاذب للحصول على شهادة تصديق إلكترونية موصوفة، سواء أتحققت النتيجة (الحصول على الشهادة) أم لا، ما دام الإقرار الكاذب قد تم بغية الحصول عليها، وهذا هو الركن المادي للجريمة، أما الركن المعنوي فيتمثل في القصد العام بعنصريه العلم والإرادة: علم الشخص بأنه يدلي بادعاء كاذب، واتجاه إرادته نحو تحقيق النتيجة، وكذلك يتوجب توافر القصد الخاص وهو نية الحصول على شهادة التصديق الإلكتروني الموصوفة.

ولقد حددت م15 من القانون 15-04 المتطلبات القانونية التي تجعل شهادة التصديق الإلكتروني تنعت بأنها موصوفة.

6- جريمة الإخلال بالتزام الإعلام المحدد في المادتين 58 و59.

نصت م67 من القانون 15-04 سالف الذكر على عقوبة الحبس من شهرين إلى سنة واحدة، والغرامة من 200.000 إلى 1.000.000 دج أو بإحدى هاتين العقوبتين في حق كل مؤدي خدمات التصديق الإلكتروني أخل بالتزام إعلام السلطة الاقتصادية بالتوقف عن نشاطه في الآجال المحددة في المادتين 58 و59 من هذا القانون، وحسب هاتين المادتين، هنالك تفرقة بين رغبة

مؤدي خدمات التصديق في التوقف عن نشاطه بإرادته (م58)، أو لأسباب خارج عن إرادته (م59)، ففي الحالة الأولى يجب عليه إعلام السلطة الاقتصادية للتصديق الالكتروني في الآجال المحددة في سياسة التصديق لهذه السلطة عن رغبته بالتوقف، ويواصل تقديم الخدمة إلى غاية البث في طلبه، وفي الحالة الثانية يجب عليه إعلام السلطة فورا، وتقوم هذه الأخيرة بإلغاء شهادته للتصديق الإلكتروني الموصوفة، ويجب على مؤدي الخدمة اتخاذ كل التدابير اللازمة من أجل حفظ المعلومات المرتبطة بشهادة التصديق الإلكتروني الموصوفة الممنوحة له.

الملاحظ أن العقوبة تطال مؤدي الخدمة في حالة الإخلال بالتزام الإعلام، ولم تتطرق إلى جزاءات الإخلال بالالتزامات الأخرى المقررة في المادتين المذكورتين أعلاه، وخاصة ضمان الاستمرار في الخدمة، وحفظ المعلومات المرتبطة بشهادة التصديق الإلكتروني الموصوفة.

7- جريمة حيازة أو إفشاء أو استعمال بيانات إنشاء توقيع إلكتروني موصوف.

نصت على هذه الجريمة م68 من القانون 15-04 المذكور آنفا، والتي عاقبت بالحبس من ثلاثة أشهر إلى ثلاث سنوات والغرامة من مليون إلى خمسة ملايين دينار أو بإحدى العقوبتين كل من يقوم بحيازة أو إفشاء أو استعمال بيانات إنشاء توقيع إلكتروني موصوف خاصة بالغير.

عرفت م3/2 من القانون 15-04 سالف الذكر المقصود ببيانات إنشاء التوقيع الإلكتروني، بأنها بيانات فريدة، مثل الرموز أو مفاتيح التشفير الخاصة التي يستعملها الموقع لإنشاء التوقيع الإلكتروني.

الركن المادي لهذه الجريمة له ثلاثة صور: الأولى هي حيازة بيانات إنشاء توقيع إلكتروني خاص بالغير، وبديهي كي تقوم الجريمة أن تكون الحيازة غير قانونية، ويستوي بعد ذلك الطريقة التي حصل بها الحائز على البيانات، سواء عن طريق الغش والاحتيال أو عن طريق آخر، كأن يعثر على قرص مرن لشخص ما به هذه البيانات ولا يقوم بإعادته لصاحبه بل يحتفظ به بنية استعماله، فالمعيار هنا أن تكون الحيازة ضد إرادة صاحبها، أو ضد التزام قانوني أو عقدي، أما الصورة الثانية فهي إفشاء بيانات إنشاء التوقيع الإلكتروني، والفرض هنا أن يكون مطلعا على هذه البيانات ويفشيها للغير، كأن يكون صاحبها قد عهد به إليها على سبيل الأمانة، أما الصورة الثالثة فهي استعمال بيانات إنشاء التوقيع الإلكتروني الموصوف الخاص بالغير دون وجه حق، ولكن هل يشترط وقوع

الضرر في حق صاحب التوقيع الموصوف أم لا؟ إن المصلحة المحمية هي ثقة التوقيع الإلكتروني وليس صاحب التوقيع في حد ذاته، ولذلك تقوم الجريمة حتى ولو لم يلحق ضرر بصاحب التوقيع، كما أن نص المادة لم يشر إلى الضرر، وبالتالي لا ينبغي اشتراط أمر لم يشترطه المشرع.

وحسب النص يمكن أن تقوم هذه الجريمة أيضا في حق مزود خدمة التصديق، خاصة وأن م48 من القانون 15-04 سالف الذكر نصت على عدم جواز مؤدي خدمات التصديق الإلكتروني حفظ أو نسخ بيانات إنشاء توقيع الشخص الذي منحت له شهادة التصديق الإلكتروني الموصوفة.

ويفترض لقيام الجريمة حسب القواعد العامة توافر القصد العام دون القصد الخاص.

8- جريمة انتهاك سرية وخصوصية البيانات.

نصت م70 من القانون 15-04 سالف الذكر على عقوبة الحبس من ثلاثة أشهر إلى سنتين، والغرامة من مائتي ألف إلى مليون دينار أو بإحدى العقوبتين في حق مؤدي خدمات التصديق الإلكتروني الذين يخلون بسرية البيانات والمعلومات المتعلقة بشهادات التصديق الإلكتروني، كما نصت م71 من القانون ذاته على العقوبة من ستة أشهر إلى ثلاث سنوات، والغرامة من مائتي ألف إلى مليون دينار أو بإحدى هاتين العقوبتين في حق مؤدي خدمات التصديق الإلكتروني الذين يقومون بجمع البيانات الشخصية للمعني دون موافقته الصريحة، أو جمع بيانات شخصية غير ضرورية لمنح وحفظ شهادة التصديق الإلكتروني، أو استعمال البيانات الشخصية لأغراض غير تلك المحددة قانونا.

هاتان المادتان هدفهما الحفاظ على البيانات الشخصية للأفراد، وعدم انتهاك خصوصياتهم، فالمادة الأولى تتحدث عن واجب الحفاظ على سرية المعلومات والبيانات، بينما تضع الثانية مجموعة من الضوابط لحماية البيانات الشخصية للأفراد، ومن أخطرها أن يقوم مزود الخدمة بتكوين قاعدة بيانات عن الشخص بأن يطلب منه معلومات غير مطلوبة قانونا، سواء كان ينوي استعمالها لأغراض إجرامية أو لمجرد الفضول.

ونص المشرع المصري أيضا في مشروع قانون التجارة الإلكترونية على جريمة انتهاك سرية وخصوصية البيانات، وإن كانت تختلف عن الجريمتين الواردتين في القانون الجزائري، إلا أنهما تتفقان من حيث محل الجريمة، حيث عاقب المشرع المصري كل من يقوم بفض معلومات مشفرة في غير

الأحوال المصرح بها قانونا، ويتحقق الركن المادي للجريمة بمجرد انتهاك سرية البيانات وخصوصياتها حتى ولو لم يترتب على الفعل أية نتيجة، فالجريمة سلوكية لا تشترط تحقق النتيجة.[1]

9- جريمة مزاولة نشاط التوقيع الإلكتروني دون ترخيص.

نصت م72 من القانون 15-04 سالف الذكر على عقوبة الحبس من سنة إلى ثلاث سنوات، والغرامة من مائتي ألف إلى مليوني دينار أو بإحدى العقوبتين في حق من يؤدي خدمات التصديق الإلكتروني دون ترخيص، أو يستأنف أو يواصل نشاطه بعد سحب الترخيص منه، كما نصت المادة على عقوبة تكميلية هي مصادرة التجهيزات المستعملة في ارتكاب الجريمة.

ولا بد من الحصول على ترخيص من السلطة الاقتصادية للتصديق الالكتروني المنصوص عليها في م29، والتي حددت مهامها م30 من القانون 15-04 سالف الذكر.

ورد النص على هذه الجريمة أيضا في نص م23/د من التشريع المصري 15 لسنة 2004، والملاحظ أن المشرع المصري في م23 من قانون التوقيع الإلكتروني ينص فقط على صورة واحدة وهي مزاولة النشاط دون ترخيص دون التطرق إلى من كان مرخصا ثم سحبت منه الشهادة، وربما كان مصيبا في ذلك باعتبار أن من كان مرخصا وسحبت منه الرخصة يعتبر في حكم من قام يزاول المهنة دون ترخيص، اللهم إلا إذا لم يكن عالما بسحب الترخيص، ففي هذه الحالة لا تقوم الجريمة في حقه لانتفاء أحد عنصري القصد الجنائي وهو العلم.

غير أن المشرع المصري وقع في أمر معيب في م23/أ من التشريع السابق إذ نص أيضا على معاقبة من يصدر شهادة تصديق إلكتروني دون ترخيص، مما يراه البعض تجريما بنصين تشريعين على السلوك الإجرامي ذاته.[2]

تقوم الجريمة بقيام المؤسسة أو الفرد بإصدار شهادة تصديق إلكترونية دون ترخيص، أي أنه زاول فعل الإصدار فعلا، أما لو كان مجرد إعلان عن نيته في الإصدار فلا تقوم الجريمة، إذ ينبغي

[1] أيمن رمضان، المرجع السابق، ص140.

[2] المرجع نفسه، ص137.

لقيام الجريمة صدور الشهادة فعلا. والملاحظ من صياغة المادة أنها عمدية يجب لتوافرها القصد العام دون القصد الخاص.[1]

ويرى الفقه بأن مزود الخدمات الذي يتقاعس عن سداد رسم الترخيص، أو يتنازل عن رخصته للغير، أو يتوقف عن نشاطه المرخص له به، أو يندمج مع آخر دون الحصول على موافقة كتابية من الهيئة مانحة التراخيص (هيئة تنمية صناعة تكنولوجيا المعلومات) تطبق عليه أحكام المادة 23/د من القانون 2004/15 المصري، ويرى البعض أن مخالفة إجراء من الإجراءات أو الضوابط التي ينص عليها في اللائحة التنفيذية للقانون بهذا الشأن يرتب المعاقبة الجنائية حسب هذا النص.[2]

10- جريمة إفشاء أسرار المهنة

عاقبت م74 من القانون 15-04 بالحبس من ثلاثة أشهر إلى سنتين، والغرامة من ألفي إلى مائتي ألف دينار أو بهاتين العقوبتين فقط المكلف بالتدقيق الذي يكشف معلومات سرية اطلع عليها أثناء قيامه بالتدقيق.

هذه المادة أيضا تحمي خصوصية الأفراد من حيث عدم جواز إفشاء الأسرار المتعلقة بهم، ولكن محلها يختلف، فهنا محل الجريمة هو الأسرار، بينما محل جريمة م70 هو البيانات الشخصية ولو لم تكن سرية.

وهذه الجريمة قريبة من جريمة إفشاء أسرار المهنة المنصوص عليها في م301 ق ع، إلا أنها تختلف عنها في أن حصول المدقق على المعلومات السرية يكون بفعل إيجابي، أي أثناء القيام بعملية التحقق، وقد تكون هذه المعلومات موثقة.

وقد أعطى المشرع في م16/2 من القانون 15-04 تعريفا للتدقيق بأنه التحقق من مدى المطابقة وفقا لمرجعية ما.

نص المشرع الجزائري أيضا على جريمة استعمال الشخص لشهادة إلكترونية موصوفة لغير الأغراض التي منحت من أجلها، والفرض هنا أن الحصول على الشهادة كان قانونيا، لكن استعمالها

[1] الكعبي، المرجع السابق، ص513.

[2] أيمن رمضان، المرجع السابق، ص137.

كان في غير الأغراض التي منحت من أجلها، أيا كان هذا الاستعمال، وأيا كان الدافع من ورائه، فالعبرة بالاستعمال غير المشروع، وعقوبة هذه الجريمة حسب م74 هي الغرامة التي قد تصل حتى مائتي ألف دينار.

نص المشرع الجزائري على مبدأ عقاب الشخص المعنوي الذي ارتكب إحدى الجرائم المنصوص عليها في المواد 66-74 من القانون 15-04 بغرامة تعادل خمس مرات الحد الأقصى للغرامة المنصوص عليها بالنسبة للشخص الطبيعي.

المبحث الثاني: الحماية الجزائية للحق في الخصوصية للمستهلك الإلكتروني.

من المواضيع الأكثر إثارة للجدل موضوع الحق في الخصوصية، الذي اعترفت به الدساتير والقوانين الوطنية بالإضافة إلى المواثيق الدولية، وهو ما يعرف أيضا بالحياة الخاصة، وهي فكرة عصرية، ظهرت حديثا وانتقلت من الجانب الأخلاقي إلى الجانب القانوني الذي يعمل على صونها وحمايتها، وتصدى الكثير من الفقهاء لتعريفها ووضع أطرها، إلا أنهم لم يتفقوا على تعريف جامع مانع لها، وإن اتفقوا حول عناصرها، وأنها مرتبطة بالشخص، وكل ماله علاقة شخصية به كمحل إقامته أو اسمه أو عائلته، وكذا بروتوكول الانترنت الخاص به (IP) وما إلى ذلك؛[1] هذه الخصوصية قد تتعرض للاعتداء خاصة فيما يتعلق بالبيانات عند التعامل في التجارة الإلكترونية، لأن طبيعة هذه التجارة تقتضي أن يدلي المستهلك ببعض المعلومات الشخصية لإتمام المعاملة؛ وتقوم هنا أيضا مسؤولية مزودي الخدمة في عدم التعدي على الحق في الخصوصية (وكل اعتداء غير مشروع على الشبكة)، بل وحمايتها من اعتداء الغير عليها.

يتم التطرق إلى حماية الحياة الخاصة للمستهلك الإلكتروني (المطلب الأول)، ثم المسؤولية الجزائية لمقدمي الخدمات الوسيطة عن الانتهاكات التي قد تحدث أثناء أو بسبب المعاملات الإلكترونية المختلفة (المطلب الثاني).

[1] Roseline Letteron, libertés publiques, Dalloz, Paris 2012, p368-369.

المطلب الأول: الحماية الجزائية للبيانات الشخصية.

من الطبيعي أن يتم أثناء إجراء المعاملات الإلكترونية تبادل بيانات الأشخاص، منها ما يتعلق بالعملاء، ومنها ما يتعلق بالعاملين بالمشروع، كالبيانات المتعلقة بالموظفين والقائمين على الإدارة، وهذا الأمر يستوجب توفير حماية قانونية لازمة للمستهلك عند قيامه بالتعاقد الإلكتروني، ومن أهمها حماية المستهلك من الاطلاع على بياناته الاسمية أو الشخصية التي يدلي بها بصورة مباشرة أو غير مباشرة قبل أو أثناء عملية إبرام العقد، أو عن طريق تتبع استخدامه للانترنت.[1]

والبيانات الشخصية حسب بعض الفقه الفرنسي هي تلك البيانات المتعلقة بالحياة الخاصة بالفرد كتلك المتعلقة بحالته الصحية والمالية والمهنية والوظيفية والعائلية، وهي تلك البيانات التي يحميها المشرع بمقتضى المادة التاسعة من القانون المدني الفرنسي، أي تلك المتصلة بحرمة الحياة الخاصة، ويذهب البعض أبعد من ذلك في تحديد مفهوم البيانات الشخصية بأنها أيضا كل ما يسمح برسم صورة لاتجاهات الشخص وميولاته السياسية والدينية وتعاملاته المالية والبنكية، وجنسيته وهواياته.

فيما يتعلق بالانترنت، وخاصة المواقع الاجتماعية، تبدو الأمور معقدة بعض الشيء، غير أن هنالك مبدأين ينبغي احترامهما: الحق في الهوية الرقمية(le droit à l'identité numérique)، والحق في النسيان الرقمي(le droit à l'oubli numérique)؛[2] فالمبدأ الأول يعني مجموعة المعطيات التي يضعها مستعمل الانترنت، على مواقع الانترنت، ويسمح له هذا الحق، بتسيير هذه المعطيات وضمان سريتها إذا رغب في ذلك، ويثور السؤال هنا: هل يعتبر غصب الهوية الرقمية جريمة يعاقب عليها القانون؟ لا يعتبر هذا الفعل حاليا جريمة في حد ذاتها، بل "جنحة تحضيرية" لارتكاب جنح أخرى، بمعنى أن غصب الهوية الرقمية غير معاقب عليه حاليا إلا إذا ارتكب المغتصب جرائم أخرى، بيد أن فعل الغصب قد يشكل جنحة مستقلة عن قريب، كما هو الأمر بالنسبة لمجرد الولوج غير المشروع.[3]

---

[1] مدحت عبد الحليم رمضان، المرجع السابق، ص75.

[2] Roseline Letteron, op cit, p385.

[3] Mathieu Prud'homme, l'usurpation d'identité numérique: bientôt un nouveau délit, Gazette du palais 2, Mars Avril 2010, p777.

أما المبدأ الثاني فيرمي إلى محو المعطيات المتعلقة بالشخص والموجودة على مواقع الانترنت إذا رغب في ذلك، وأيضا ضرورة قيام مسيري مواقع الانترنت بمحو هذه المعطيات بعد مرور مدة زمنية معينة، وهما يشكلان الحق في محو الآثار، لذا وفي غياب نصوص قانونية حول هذه النقطة، وضعت مؤسسة (Google) في الفاتح أبريل 2012 قواعد جديدة للسرية لفائدة مستعمليها، تتعهد باحترامها، كما تعهدت بالتعاون مع السلطات المحلية المكلفة بإدارة المعطيات، وهو ما يعني بوضوح بأنها لا تنوي الارتباط بقوانين الدول التي تبث فيها المعطيات، ولكن فقط بقانون الو م أ.[1]

وقد نظم القانون الفرنسي، وبعض القوانين المقارنة، عملية معالجة البيانات الشخصية واستعمالها، ويقصد بالمعالجة مجموعة من العمليات تتم بوسيلة آلية بجمع وتسجيل وإعداد وتعديل وحفظ وإهلاك المعلومات الاسمية.[2]

عموما إن موضوع الحياة الخاصة في علاقته بالانترنت يدور حول ستة محاور رئيسة هي: المعلومة، الرضا، التعديل أو التغيير، التبرير، الاحتفاظ ونقل البيانات.[3]

ومن الفقه من صنف هذه الجرائم إلى أربع فئات، وهي الجرائم الماسة بالحق في الحياة الشخصية من الناحية الموضوعية، الجرائم المنطوية على مخالفة القواعد الإجرائية المنظمة لأنشطة المعالجة الآلية للبيانات الشخصية، الجرائم الماسة بحق الشخص في الإحاطة بالبيانات المتعلقة به، وأخيرا إهمال الإجراءات الأمنية، كما أورد الفقيه (Ulrich Siber) صور انتهاك الخصوصية المتصلة بالمعالجة الآلية للبيانات الشخصية اعتمادا على نوعية الأساليب الإجرامية المستخدمة.[4]

بناء على ما تقدم يتم معالجة هذا المطلب من خلال التطرق إلى الحماية الجزائية للبيانات الشخصية في القانون الفرنسي (الفرع الأول)، وفي القانون الجزائري وبعض القوانين العربية الأخرى (الفرع الثاني).

---

[1] Roseline Letteron, op cit, p387.

[2] مدحت عبد الحليم رمضان، المرجع السابق، ص73.

[3] Mme kheira Dari Bekara, protection des données personnelles coté utilisateur dans le e commerce, thèse de doctorat conjoint Télecom Sud Paris et l'université Pierre et Marie Curie , Paris 2012, p42-45.

[4] د. بولين أنطنيوس أيوب، الحماية القانونية للحياة الشخصية في مجال المعلوماتية، منشورات الحلبي الحقوقية، عمان الأردن (دون ذكر سنة النشر)، ص388.

الفرع الأول: الحماية الجزائية للبيانات الشخصية في القانون الفرنسي

يتطلب القانون الفرنسي المسمى "المعلوماتية والحرية" عند معالجة أي بيانات اسمية شخصية من قبل أشخاص القانون الخاص إخطار اللجنة القومية للمعلوماتية والحريات، ويتطلب الحصول على تصريح مسبق إذا كان من يقوم بجمع المعلومات أحد أشخاص القانون العام أو أحد أشخاص القانون الخاص العاملين لحساب الدولة.[1]

وإذا رغب القائمون على موقع من مواقع الانترنت التعامل مع البيانات الشخصية تعين عليهم إخطار اللجنة الوطنية للمعلوماتية والحريات(CNIL)[2] مسبقا، وإخطار المواطنين بالمخاطر المترتبة عن وضع بياناتهم الشخصية بموقع الانترنت، وحقهم في الاعتراض في أي وقت على نشر هذه البيانات، وحقهم أيضا في الاعتراض والتصحيح ومحو البيانات لأسباب مشروعة.

ويتعين أيضا عند الرغبة في استخدام نظام "الكعك المحلى" إخطار اللجنة، لأنه يمكن عن طريق هذا النظام معرفة معلومات عن المستهلك تتعلق بالمواقع التي تصفحها والأشياء التي بحث عنها والوقت المفضل لديه للإبحار في الانترنت، وميوله الشخصية، وبالتالي يمكن معالجة هذه المعلومات ووضعها على قاعدة للبيانات لاستخدامها.

وقد ساهم القضاء الفرنسي في تحديد مفهوم البيانات الاسمية التي يوفر لها القانون الحماية ومن ذلك رقم الهاتف، والمعلومات الخاصة بجنسية سكان عقار من العقارات والبيانات الخاصة بالأفكار الفلسفية للمشتركين ببعض الدوريات، ولقد أدين أحد الأشخاص لقيامه بوضع صور عارية لخليلته السابقة على موقعه للانترنت.[3]

وفي جويلية 1998 وضعت اللجنة القومية للمعلوماتية والحريات نموذجا لطلب معالجة البيانات الاسمية على مواقع الانترنت.

واعتبرت اللجنة من قبيل معالجة البيانات الاسمية الاستبيان الاختياري أو الإجباري، الذي يتعين على المتصفح استكماله للانتقال إلى مكان آخر على الموقع، كما اعتبرت كذلك من

---

[1] عبد الحليم رمضان، المرجع السابق، ص85.

[2] Commission nationale de l'informatique et des libertés.

[3] عبد الحليم رمضان، المرجع السابق، ص86.

قبيل معالجة البيانات الاسمية عملية تتبع الأثر التي يقوم بها مورد الخدمة، والتي يتعرف من خلالها على المواقع التي تصفحها العميل ووقت وتاريخ التصفح، ويقوم بتخزين هذه البيانات لمدة من الزمن وتحديد شخصية العميل، ونظرت اللجنة موضوع "الكعك المحلى" الذي يوضع على الاسطوانة الصلبة لجهاز الكمبيوتر الخاص بالعميل دون علمه، فيسمح بمعرفة شخصيته وهواياته، وأوجبت ضرورة إخطار المستخدمين بوضع "الكعك المحلى" على أجهزتهم بما يسمح لهم بالاعتراض على ذلك.[1]

وعليه، يتم تناول أهم الجرائم التي تطرق إليها المشرع الفرنسي في "قانون المعلوماتية والحرية" والذي أدرجت مواده في قانون العقوبات، وقد قصر المشرع الفرنسي نطاق حماية البيانات على الأشخاص الطبيعية دون المعنوية،[2] ولا يشاطره في ذلك تشريعات أوربية أخرى كالنرويج والنمسا وايرلندا ولوكسمبورغ والدانمرك.[3]

أكدت CNIL على أن القواعد الواردة بقانون 1978 تنطبق على الانترنت.[4]

أولا: جريمة عدم اتخاذ الإجراءات الأولية لإجراء معالجة البيانات.

بالاطلاع على نص المادة 41 من قانون السادس من يناير 1978 وكذا المواد 15 و16 و17 من القانون السابق، يمكن القول أن معالجة البيانات لحساب الحكومة يتطلب ترخيصا، والمعالجات التي تتم لحساب القانون الخاص يكتفى فيها بإخطار اللجنة الوطنية للمعلوماتية والحريات، وإذا كانت المعالجة لحساب أشخاص القانون العام أو الخاص ولا تنطوي على مساس بالحياة الخاصة أو الحريات وتتسق مع الضوابط الموضوعة من طرف اللجنة اكتفي بشأنها بإخطار مبسط للجنة.

وأعاد المشرع صياغة نص م41 من القانون المذكور آنفا، وضمنها المادة 226-16 ق ع ف[5] بحيث تنص على معاقبة كل من يقوم ولو بإهمال بمعالجة إلكترونية للبيانات الاسمية دون مراعاة للإجراءات الأولية للقيام بها.

---

[1] عبد الحليم رمضان، المرجع السابق، ص88.

[2] الشوابكة، المرجع السابق، ص84.

[3] غنام محمد غنام، المرجع السابق، ص100.

[4] الشوابكة، المرجع السابق، ص85.

[5] Le fait, y compris par négligence, de procéder ou de faire procéder à des traitements de données à caractère personnel sans qu'aient été respectées les formalités préalables à leur mise en oeuvre prévues par la loi est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende. Est puni des mêmes peines le fait, y compris par

وقد أدى هذا إلى التساؤل عما إذا كان المقصود من عدم مراعاة الإجراءات الأولية هو عدم مراعاة الإجراءات الواردة بالمادتين 15 و16 أم يمتد ليشمل عدم مراعاة الإجراءات المنصوص عليها بالمادة 17، وانتهى جانب من الفقه إلى القول أن م 226-16 تمتد لتشمل عدم مراعاة أي إجراء يتطلبه القانون.[1]

ويتحقق النشاط المادي لهذه الجريمة بأي معالجة إلكترونية للبيانات الاسمية، سواء بمحوها أو تعديلها أو تصنيفها أو حفظها... دون اتخاذ الإجراءات الأولية التي يتطلبها القانون، أي دون الحصول على إذن من CNIL،[2] كما يعاقب من أمر بإجراء المعالجة بالعقوبة نفسها المقررة لمن يقوم بالمعالجة كفاعلين أصليين للجريمة، حيث أن المشرع الفرنسي لم يميز بينهما.

واعتبرت محكمة النقض الفرنسية هذه الجريمة من الجرائم المادية التي يفترض توافر القصد الجنائي فيها بمجرد ارتكاب الفعل المادي، خلافا لما انتهى إليه قضاء الموضوع الذي تطلب توافر القصد الجنائي لدى الجاني.

ويرى جانب من الفقه بأن م121-3/1 ق ع ف أكدت صراحة عدم قيام الركن المعنوي للجريمة دون إرادة، بما يعني عدم صحة القول بافتراض المسؤولية الجنائية، وعليه فإن المشرع يتطلب توافر الركن المعنوي للجريمة سواء كان هناك عمد أم خطأ،[3] ومما يؤيد هذا الرأي أن تعبير "ولو بإهمال" جعل مسألة اشتراط الركن المعنوي محسومة، حيث نستنتج أن المشرع اعتبر الإهمال كحد أدنى للعنصر النفسي لدى الجاني، ولو كان المشرع يريد افتراض توافر القصد الجنائي لما جاء بهذا التعبير.[4] وأكدت محكمة النقض الفرنسية أن هذه الجريمة من الجرائم المادية، يفترض توافر القصد الجنائي فيها بمجرد ارتكاب الفعل.[5]

---

négligence, de procéder ou de faire procéder à un traitement qui a fait l'objet de l'une des mesures prévues au 2° du I de l'article 45 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

[1] مدحت عبد الحليم رمضان. المرجع السابق. ص94.

[2] الشوابكة، المرجع السابق، ص ص87-88.

[3] مدحت عبد الحليم رمضان، المرجع السابق،ص 95.

[4] أمين اعزان، المرجع السابق، ص 196.

[5] الشوابكة، المرجع السابق، ص88.

أضاف المشرع الفرنسي [1] Art. 226-16-1-A لتجريم وعقاب على عدم احترام المقاييس والقواعد القانونية المحددة في قانون 1978 والموضوعة من قبلCNIL ولو كان ذلك عن طريق الإهمال، بالعقوبات ذاتها المقررة للجريمة السابقة، كما عاقبت Art. 226-16-1 بالعقوبة ذاتها كل من يقوم بمعالجة إلكترونية لبيانات اسمية تحمل رقم تسجيل الأشخاص في السجل الوطني الخاص بهوية الأشخاص الطبيعيين.[2]

ثانيا: جريمة عدم اتخاذ الاحتياطات اللازمة لحماية البيانات المعالجة.

تنص م226-17 ق ع ف على أن يعاقب بالحبس لمدة خمس سنوات وبغرامة 300 ألف يورو من يجري أو يأمر بإجراء معالجة إلكترونية للبيانات الاسمية دون اتخاذ الاحتياطات الملائمة لحماية هذه البيانات،[3] وخصوصا للحيلولة دون تشويهها أو إتلافها أو اطلاع غير المصرح له بذلك عليها.

ويتضح من النص أن المشرع أراد أن يوفر الحماية الكافية للبيانات فعاقب على عدم اتخاذ الاحتياطات اللازمة لحماية البيانات الاسمية.

وتقع الجريمة سواء اتخذ الركن المعنوي في هذه الجريمة صورة القصد الجنائي أو الخطأ غير العمدي.[4]

عاقبت م 226-17-1 ق ع ف مزود خدمات الاتصالات الالكترونية على عدم إخطاره CNIL أو صاحب الشأن بالاعتداء الواقع على بياناته الاسمية بالعقوبات ذاتها المقررة للجريمة السابقة.[5]

---

[1] Lorsqu'il a été procédé ou fait procéder à un traitement de données à caractère personnel dans les conditions prévues par le I ou le II de l'article 24 de la loi n° 78-17 du 6 janvier 1978 précitée, le fait de ne pas respecter, y compris par négligence, les normes simplifiées ou d'exonération établies à cet effet par la Commission nationale de l'informatique et des libertés est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende.

[2] Le fait, hors les cas où le traitement a été autorisé dans les conditions prévues par la loi n° 78-17 du 6 janvier 1978 précitée, de procéder ou faire procéder à un traitement de données à caractère personnel incluant parmi les données sur lesquelles il porte le numéro d'inscription des personnes au répertoire national d'identification des personnes physiques, est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende.

[3] Le fait de procéder ou de faire procéder à un traitement de données à caractère personnel sans mettre en oeuvre les mesures prescrites à l'article 34 de la loi n° 78-17 du 6 janvier 1978 précitée est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende.

[4] مدحت عبد الحليم رمضان، المرجع السابق، ص96.

[5] Le fait pour un fournisseur de services de communications électroniques de ne pas procéder à la notification d'une violation de données à caractère personnel à la Commission nationale de l'informatique et des libertés ou à

واضح من النص أنه يفترض علم مزود الخدمة بالاعتداء، ورغم ذلك لا يقوم بإبلاغ CNIL أو صاحب الشأن.

ثالثا: جريمة المعالجة غير المشروعة للبيانات.

نصت م226-18 ق ع ف[1] على معاقبة كل من يقوم بجمع معطيات اسمية بصورة غير مشروعة أو غير نبيلة، أو عن طريق الغش تتعلق بشخص طبيعي، كما نصت م226-18-1 على معاقبة من يقوم بجمع بيانات خاصة لشخص طبيعي إذا تعلق الأمر بالأبحاث بما في ذلك التجارية، أو أبدى الشخص اعتراضه، وكان الاعتراض يقوم على أسباب مشروعة،[2] بالحبس لمدة خمس سنوات وغرامة 300 ألف يورو.

وحسب القضاء الفرنسي، لا تقوم هذه الجريمة إلا إذا تم تسجيل البيانات بعد جمعها، والاحتفاظ بها في "فيش" أو معالجتها بالحاسب الآلي.[3]

والجرائم المشار إليها في هذه المادة (226-18 ق ع ف) من الجرائم العمدية، أي التي تتطلب لقيامها توافر القصد الجنائي بعنصريه العلم والإرادة.

رابعا: جريمة تسجيل وحفظ بيانات شخصية أو بيانات تتعلق بالماضي لأشخاص مصنفين.

من خلال نص م226-19 ق ع ف (المقابلة للمادة 31 من قانون 1978) عاقب المشرع الفرنسي بالحبس لمدة خمس سنوات والغرامة 300 ألف يورو عملية وضع أو حفظ بذاكرة إلكترونية دون موافقة صريحة من قبل صاحب الشأن، بيانات اسمية تظهر بصورة مباشرة أو غير مباشرة أصوله العرقية أو معتقداته السياسية أو الفلسفية أو الدينية أو انتماءاته النقابية أو تتعلق

---

l'intéressé, en méconnaissance des dispositions du II de l'article 34 bis de la loi n° 78-17 du 6 janvier 1978, est puni de cinq ans d'emprisonnement et de 300 000 € d'amende

[1] Le fait de collecter des données à caractère personnel par un moyen frauduleux, déloyal ou illicite est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende.

[2] Le fait de procéder à un traitement de données à caractère personnel concernant une personne physique malgré l'opposition de cette personne, lorsque ce traitement répond à des fins de prospection, notamment commerciale, ou lorsque cette opposition est fondée sur des motifs légitimes, est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende.

[3] غنام محمد غنام، المرجع السابق، ص120.

بأخلاقه، كما يعاقب بالعقوبة ذاتها من يقوم في غير الحالات التي يقررها القانون بوضع أو حفظ بيانات اسمية في ذاكرة إلكترونية تتعلق بالجرائم أو أحكام الإدانة أو التدابير.[1]

يرى جانب من الفقه أن تعبير أحكام الإدانة يشمل أيضا أي تقرير للجرائم ومباشرة الدعوى العمومية بشأنها طالما أن معالجة البيانات تمت دون تصريح قانوني.[2]

نصت م226-19-1 ق ع ف،[3] على جريمة معالجة بيانات اسمية هدفها البحث في المجال الصحي دون احترام الوسائل القانونية، ومنها إخطار أصحاب الشأن مسبقا بحقهم في الاعتراض أو التعديل بطبيعة المعطيات ووجهتها، أو رغم معارضة الشخص المعني، أو في غياب موافقة صريحة من المعني عندما يتطلب القانون مثل هذه الموافقة الصريحة، أو عندما يتعلق الأمر بشخص توفي، وكان يرفض مثل هذه المعالجة لبياناته الشخصية.

خامسا: جريمة حفظ بيانات شخصية خارج الوقت المصرح به وفقا للطلب أو الإعلان السابق.

تعاقب م226-20 ق ع ف[4] بالحبس خمس سنوات والغرامة 300 ألف يورو كل شخص قام بدون موافقة اللجنة الوطنية للمعلوماتية والحريات بحفظ معلومات اسمية بما يجاوز الوقت المحدد في طلب الموافقة أو الإخطار السابق على عملية الحفظ، إلا إذا كان الحفظ لأغراض تاريخية أو

[1] Le fait, hors les cas prévus par la loi, de mettre ou de conserver en mémoire informatisée, sans le consentement exprès de l'intéressé, des données à caractère personnel qui, directement ou indirectement, font apparaître les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses, ou les appartenances syndicales des personnes, ou qui sont relatives à la santé ou à l'orientation ou identité sexuelle de celles-ci, est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende. Est puni des mêmes peines le fait, hors les cas prévus par la loi, de mettre ou de conserver en mémoire informatisée des données à caractère personnel concernant des infractions, des condamnations ou des mesures de sûreté.

[2] عبد الحليم رمضان، المرجع السابق، ص101.

[3] En cas de traitement de données à caractère personnel ayant pour fin la recherche dans le domaine de la santé, est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende le fait de procéder à un traitement : 1° Sans avoir préalablement informé individuellement les personnes sur le compte desquelles des données à caractère personnel sont recueillies ou transmises de leur droit d'accès, de rectification et d'opposition, de la nature des données transmises et des destinataires de celles-ci ; 2° Malgré l'opposition de la personne concernée ou, lorsqu'il est prévu par la loi, en l'absence du consentement éclairé et exprès de la personne, ou s'il s'agit d'une personne décédée, malgré le refus exprimé par celle-ci de son vivant.

[4] Le fait de conserver des données à caractère personnel au-delà de la durée prévue par la loi ou le règlement, par la demande d'autorisation ou d'avis, ou par la déclaration préalable adressée à la Commission nationale de l'informatique et des libertés, est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende, sauf si cette conservation est effectuée à des fins historiques, statistiques ou scientifiques dans les conditions prévues par la loi. Est puni des mêmes peines le fait, hors les cas prévus par la loi, de traiter à des fins autres qu'historiques, statistiques ou scientifiques des données à caractère personnel conservées au-delà de la durée mentionnée au premier alinéa.

إحصائية أو علمية ووفقا لما يتطلبه القانون، كما يعاقب القانون على معالجة معطيات (غير تلك الهادفة لأغراض علمية...) تم حفظها حفظا تجاوز المدة القانونية.

وبناء عليه تقع الجريمة إذا كانت عملية المعالجة والحفظ قد تمت وفقا لأحكام القانون ولكن تم حفظ هذه البيانات لمدة تُجاوز المدة المطلوبة للحفظ، حفاظا على سمعة الشخص ودرءا لأي تجاوز.

سادسا: جريمة تغيير الغرض المحدد لجمع البيانات الاسمية.

تعاقب م 226-21 ق ع ف[1] بالعقوبات السابقة كل من يحوز بيانات اسمية بمناسبة قيامه بتسجيلها أو تصنيفها أو نقلها أو أي إجراء آخر من أوجه المعالجة، إذا غير من الوجهة النهائية المقررة لهذه البيانات وفقا للقانون أو القرار الصادر بشأنها أو في الإخطار السابق عن القيام بالمعالجة.

يتحقق النشاط المادي لهذه الجريمة بمجرد الانحراف عن الغاية أو الهدف المتوخى من المعالجة الآلية للمعطيات، ويفترض هذا الأمر الحصول على هذه المعطيات بصورة مشروعة، أي بإذن من CNIL، بيد أن الفاعل ينحرف عن الهدف المقصود منها.[2]

تحديد الغرض أو الغاية من إجراء المعالجة الإلكترونية مسبقا، يهدف إلى فرض الرقابة من قبلCNIL لتجنب إساءة استخدام المعطيات، دون الحد من الإمكانيات المتاحة لاستغلالها.[3]

الركن المعنوي في هذه الجريمة يتخذ صورة القصد الجنائي العام، بعنصريه العلم والإرادة، علم الجاني بأن فعله يشكل انحرافا عن الغاية من المعالجة الإلكترونية للمعطيات الاسمية، وانصراف إرادته رغم ذلك لتحقيق فعله غير المشروع.[4]

---

[1] Le fait, par toute personne détentrice de données à caractère personnel à l'occasion de leur enregistrement, de leur classement, de leur transmission ou de toute autre forme de traitement, de détourner ces informations de leur finalité telle que définie par la disposition législative, l'acte réglementaire ou la décision de la Commission nationale de l'informatique et des libertés autorisant le traitement automatisé, ou par les déclarations préalables à la mise en oeuvre de ce traitement, est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende.

[2] الشوابكة، المرجع السابق، ص99.

[3] المرجع نفسه، ص100.

[4] المرجع نفسه، ص100.

سابعا: جريمة الإفشاء غير المشروع للبيانات الاسمية

نصت عليها م226-22 ق ع ف التي عاقبت بالعقوبات السالفة كل فعل يرتكبه شخص قام بالكشف عن بيانات اسمية بمناسبة تسجيل أو فهرسة أو نقل أي شكل من أشكال معالجة البيانات الاسمية والتي 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 أية صفة في تلقي هذه المعلومات.[1]

وتخفض العقوبة إلى الحبس لمدة سنة والغرامة لمائة ألف يورو إذا وقعت الجريمة نتيجة عدم الاحتياط أو الإهمال.[2]

ولا تحرك الدعوى الجنائية إلا بناء على شكوى من الضحية أو ممثله القانوني، أو أصحاب الشأن.[3]

يتحقق النشاط المادي لهذه الجريمة في صورتين: - حيازة البيانات الاسمية، - إفشاؤها للغير ممن ليس لهم حق الاطلاع عليها دون موافقة صريحة من صاحب الشأن، مما يلحق ضررا به يمس شرفه أو اعتباره.[4]

فإذا كانت البيانات الشخصية عن الفرد تتمثل في بيانات عن حالته العائلية، أودعها صاحبها عند إحدى الوكالات المتخصصة في التعرف بين الجنسين (قد يكون ذلك عبر الانترنت) بغرض الزواج، وحدث انقسام للشركة إلى شركتين، فإن وجود هذه البيانات لدى الشركة الوليدة لا

---

[1] Le fait, par toute personne qui a recueilli, à l'occasion de leur enregistrement, de leur classement, de leur transmission ou d'une autre forme de traitement, des données à caractère personnel dont la divulgation aurait pour effet de porter atteinte à la considération de l'intéressé ou à l'intimité de sa vie privée, de porter, sans autorisation de l'intéressé, ces données à la connaissance d'un tiers qui n'a pas qualité pour les recevoir est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende

[2] La divulgation prévue à l'alinéa précédent est punie de trois ans d'emprisonnement et de 100 000 euros d'amende lorsqu'elle a été commise par imprudence ou négligence.

[3] Dans les cas prévus aux deux alinéas précédents, la poursuite ne peut être exercée que sur plainte de la victime, de son représentant légal ou de ses ayants droit.

[4] الشوابكة، المرجع السابق، ص102.

يحقق الركن المادي في جريمة الإفشاء، لأنها ليست من الغير، هذا من جهة، ومن جهة ثانية فإن للوكالة الحق في إخبار الغير المهتم بالزواج لكي يتم التعارف بين الطرفين.[1]

وهذه الجريمة تقترب من جريمة إفشاء الأسرار (م226-13 ق ع ف)، ورغم ذلك يوجد بينهما بعض الاختلاف، حيث أن هذه الجريمة قد تنطوي على الكشف عن بيانات لا تعد من قبيل الأسرار وبالتالي فهذه الجريمة أوسع نطاقا من جريمة إفشاء الأسرار.[2]

كذلك من حيث أركان الجريمة، فإن المشرع الفرنسي في جريمة إفشاء الأسرار لا يتطلب لوقوعها أن يتم اعتداء على الشرف أو الاعتبار أو الحياة الخاصة للضحية، ولا يتصور كذلك وقوع جريمة إفشاء الأسرار إلا في صورة عمدية، بخلاف الجريمة محل الدراسة التي يمكن أن تقوم أيضا بصورة الخطأ.[3]

نصت م226-22-1 ق ع ف،[4]على معاقبة كل من يقوم، خارج الحالات المحددة قانونا، بعملية نقل بيانات اسمية، موضوع أو معدة لتكون موضوعا للمعالجة، نحو دولة لا تنتمي للمجموعة الأوربية، انتهاكا للتدابير الموضوعة من قبل لجنة المجموعة الأوربية أوCNIL بالعقوبات المقررة في الجرائم السابقة (الحبس 5 سنوات، والغرامة 300.000 يورو).

أجازت م226-22-2 ق ع ف،[5] أن يتم الأمر بمحو كل أو جزء من البيانات الاسمية موضوع المعالجة التي أوجدت الجريمة في الحالات المنصوص عليها من م226-16 إلى م 226-22-1 ق ع ف. ويسهر على مراقبة هذه العملية أعضاء CNIL.

---

[1] غنام محمد غنام، المرجع السابق، ص123.

[2] مدحت عبد الحليم رمضان، المرجع السابق، ص104.

[3] الشوابكة، المرجع السابق، ص103.

[4] Le fait, hors les cas prévus par la loi, de procéder ou de faire procéder à un transfert de données à caractère personnel faisant l'objet ou destinées à faire l'objet d'un traitement vers un Etat n'appartenant pas à la Communauté européenne en violation des mesures prises par la Commission des Communautés européennes ou par la Commission nationale de l'informatique et des libertés mentionnées à l'article 70 de la loi n° 78-17 du 6 janvier 1978 précitée est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende.

[5] Dans les cas prévus aux articles 226-16 à 226-22-1, l'effacement de tout ou partie des données à caractère personnel faisant l'objet du traitement ayant donné lieu à l'infraction peut être ordonné. Les membres et les agents de la Commission nationale de l'informatique et des libertés sont habilités à constater l'effacement de ces données.

ثامنا: جريمة التنصت على المراسلات.

قام القانون الفرنسي الصادر في العاشر من جويلية 1991 بتوفير حماية للمراسلات التي تتم بطريق وسائل الاتصالات، وقد نصت المادة 432-1/9 ق ع ف[1] على معاقبة كل شخص عام أو مكلف بخدمة عامة بالحبس والغرامة، إذا قام عند مباشرته لعمله أو بمناسبته بالأمر أو التسهيل أو القيام في غير الحالات المقررة قانونا باختلاس أو إلغاء أو فض المراسلات أو كشف محتواها.

ونصت م432-2/9 ق ع ف[2] على معاقبة كل شخص عام أو مكلف بخدمة عامة أو بأعمال استغلال خدمة الاتصالات بمقتضى م33-1 من قانون البريد والاتصالات أو بأعمال تقديم خدمة الاتصالات بالحبس والغرامة 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، وكذلك باستعمال أو بفض محتواها.

وإذا كانت الفقرة الأولى من المادة 432-9 توفر الحماية للمراسلات بمعناها الضيق بما يعني الخطابات، بدليل العبارات المستخدمة من المشرع، فإن الفقرة الثانية من ذات المادة تتعلق بالمراسلات التي تتم عبر وسائل الاتصال سواء كانت سمعية أو بصرية أو مكتوبة، وبالتالي لا تقتصر الحماية على المحادثات الهاتفية، بل تمتد لتشمل أي صورة من صور الاتصال، بما في ذلك المراسلات التي تتم عبر الانترنت، ويستوي أن تكون هذه المراسلات خاصة تتم عبر البريد الالكتروني أو مراسلات تتعلق بالتجارة الإلكترونية،[3] ولا تقتصر الحماية هنا على البيانات الاسمية فقط، بل تمتد لتشمل أي بيانات ولو لم تكن اسمية، ولو لم تتسم بالسرية، فهي بذلك حماية أشمل.

---

[1] Le fait, par une personne dépositaire de l'autorité publique ou chargée d'une mission de service public, agissant dans l'exercice ou à l'occasion de l'exercice de ses fonctions ou de sa mission, d'ordonner, de commettre ou de faciliter, hors les cas prévus par la loi, le détournement, la suppression ou l'ouverture de correspondances ou la révélation du contenu de ces correspondances, est puni de trois ans d'emprisonnement et de 45 000 euros d'amende.

[2] Est puni des mêmes peines le fait, par une personne visée à l'alinéa précédent ou un agent d'un exploitant de réseaux ouverts au public de communications électroniques ou d'un fournisseur de services de télécommunications, agissant dans l'exercice de ses fonctions, d'ordonner, de commettre ou de faciliter, hors les cas prévus par la loi, l'interception ou le détournement des correspondances émises, transmises ou reçues par la voie des télécommunications, l'utilisation ou la divulgation de leur contenu.

[3] مدحت عبد الحليم رمضان، المرجع السابق، ص106.

وإذا كانت الجريمة المنصوص عليها في م432-9/1 لا تقع إلا من الموظفين العموميين أو المكلفين بخدمة عامة والمحددين في قانون البريد فإن الجريمة المنصوص عليها في م432-9/2 تقع من الأشخاص المشار إليهم أو من أي شخص آخر مهما كانت صفته، طالما أنه يساهم في تقديم خدمات الاتصالات، والأعمال التي يجرمها نص هذه المادة هي الأمر بالتنصت على المراسلات أو اختلاسها أو القيام بذلك أو تسهيله، أو استعمالها أو فض محتواها، ويستثنى من هذه الأعمال ما أمر به القانون أو أذن به، ومنها مثلا أمر سلطات التحقيق بالكشف عن سرية هذه المراسلات.[1]

أوجدت م226-24 ق ع ف عقوبات خاصة بالأشخاص المعنوية، حسب الشروط المنصوص عليها في م121-2 ق ع ف، عند ارتكابه إحدى الجرائم السابقة، وفق ما جاء في نص م131-38 ق ع ف.

تاسعا: إعاقة مهام اللجنة الوطنية للمعلوماتية والحريات

المادة 51 المعدلة من قانون 1978 تعاقب بسنة حبسا وبغرامة قدرها 15.000 يورو فعل إعاقة مهام CNIL، سواء بالاعتراض على ممارسة مهامه الموكل بها أعضاؤه أو أعوانه المؤهلون لذلك، أم رفض تسليم هؤلاء الوثائق والمعلومات الضرورية للقيام بمهمتهم، أو تزويدهم بمعلومات ناقصة أو خاطئة.[2]

وقد تدعم دورCNIL في المراقبة منذ صدور قانون 1978، بفضل إصلاحات قانون 06 أوت 2004 المتعلق بالمعلوماتية والحريات، وعمليا قامت CNIL ب: 218 عملية مراقبة ميدانية سنة 2008، وقد يتدعم دورCNIL مستقبلا بفضل القوانين المقترحة.[3]

[1] المرجع نفسه، ص108.

[2] Céline Castets-Renard, droit de l'internet, Lextenso édition, Paris 2010, p86.

[3] Chloé Torres, renforcement des contrôles de la CNIL dans le cadre de la proposition de la loi du 06 novembre 2009, Gazette du palais1, Janvier Février, Paris 2010, p147.

الفرع الثاني: الحماية الجزائية للبيانات الشخصية في بعض التشريعات العربية

يتناول هذا الفرع، الحماية الجزائية للبيانات الشخصية في كل من مصر، تونس، والجزائر.

أولا: الحماية الجزائية للبيانات الشخصية في التشريع المصري

في مصر اقتبس المشرع المصري لفظا ومضمونا أحكام النصوص التي تكفل حماية حرمة الحياة الخاصة من قانون العقوبات الفرنسي القديم (المواد 368-372، التي تم تضمينها قانون العقوبات الفرنسي بمقتضى القانون الصادر في 17 جويلية 1970)، من خلال م309 مكرر وم309 مكررأ بمقتضى القانون رقم 37 لسنة 1972، إلا أن هذه النصوص توفر الحماية الجزائية لبعض صور الحياة الخاصة فقط (الأحاديث والصور) من أفعال معينة كالتسجيل والنشر والتصوير والتعرض لها، ولكنها لا توفر الحماية لقواعد البيانات من النسخ والاستخدام والاستغلال.[1]

وأضاف المشرع المصري مادتين جديدتين هما م21 وم22 في القانون رقم 96 لسنة 1996 المتعلق بتنظيم سلطة الصحافة، وهما تحميان الحياة الخاصة للمواطنين من تجاوزات الصحفيين.

كما أن قانون الإحصاء لسنة 1982 يحمي قواعد البيانات الخاصة بالتعداد والإحصاء.

ويثور التساؤل حول مدى إمكانية إعمال نص م310 ق ع م الخاصة **بجريمة إفشاء الأسرار على إفشاء المعلومات الاسمية المخزنة بقواعد البيانات**.

ثار جدل فقهي حول هذه المسألة، والراجح –خاصة في غياب نصوص خاصة – هو إمكانية إعمال نص هذه المادة في كثير من الحالات ومنها الحالات التي يقوم فيها الطبيب بحفظ المعلومات الخاصة بمرضاه، على قاعدة بيانات على الكمبيوتر، والمحامي الذي يحفظ معلومات تتعلق بموكليه على قاعدة بيانات، وعليه إذا أفشى الطبيب أو المحامي المعلومات المثبتة على قواعد البيانات الموجودة لديهما ارتكبا جريمة إفشاء الأسرار.[2]

ولكن هذه المادة (310 ق ع م) لا تغطي حالات أخرى لا تدخل في نطاق الأسرار، ولذلك وجب التدخل بنص خاص لحسم المشكل.

---

[1] مدحت عبد الحليم رمضان، المرجع السابق، ص110.

[2] عبد الحليم رمضان، المرجع السابق، ص115.

ثانيا: الحماية الجزائية للبيانات الشخصية في التشريع التونسي

في تونس، تضمن القانون المتعلق بحماية المعطيات الشخصية لعام 2004، جرائم تتعلق بإحالة المعطيات الشخصية المعالجة إلكترونيا، أو بعدم أخذ تدابير الحماية اللازمة عند معالجتها.

فقد اقتضى الفصل 90 من قانون 2004/07/27 أنه: "يعاقب بالسجن مدة عام، والخطية 5.000 دينار، كل من يتولى إحالة المعطيات الشخصية دون موافقة المعني بالأمر، أو موافقة الهيئة الوطنية لحماية المعطيات الشخصية في الصور المنصوص عليها في القانون".

كما حدد الفصلان 18 و19 من القانون السابق التزامات المشرف على عملية المعالجة، ومن بينها عدم وضع المعدات المستعملة في ظروف أو أماكن تمكن غير المأذون لهم الوصول إليها، عدم إمكانية قراءة السندات أو نسخها أو تعديلها أو نقلها من قبل شخص غير مأذون له بذلك، إمكانية التحقق لاحقا من هوية الأشخاص الذين نفذوا (ولجوا) إلى نظام المعلومات التي تم إقحامها، وزمن ذلك، ومن تولى ذلك...

كما حمى المشرع التونسي البيانات الاسمية في إطار قانون المبادلات والتجارة الإلكترونية لسنة 2000.

لقد اهتم المشرع التونسي بمعالجة موضوع التجارة الالكترونية معالجة تفصيلية، بهدف تغطية بها كافة جوانب الموضوع ومن ضمنها اهتمامه بتجريم الاعتداء على تداول البيانات الإلكترونية بدون ترخيص وذلك في نص م46 منه والتي تعاقب على ممارسة نشاط مورد المصادقات والوثائق الالكترونية بدون الحصول على ترخيص مسبق.

كما نصت المادة 44 من القانون التونسي على سحب الترخيص من مورد الخدمات الالكترونية وإيقاف نشاطه إذا أخل بواجباته.

يضاف إلى ذلك نص المادة 45 من القانون التي تعاقب على عدم مراعاة قواعد كراسة الشروط من جانب مورد الخدمات الالكترونية.

الركن المادي لهذه الجريمة يتوافر بمجرد تداول البيانات بدون ترخيص مسبق، حتى وإن لم يترتب على ذلك أية نتيجة إجرامية، فالجريمة تعتبر جريمة سلوكية لا تتطلب تحقيق نتيجة معينة.[1]

هذه الجريمة غير عمدية لأن الشخص قد يخطئ في تداول تلك البيانات بدون حصوله على الترخيص اللازم وبذلك يكون قد خالف اللوائح والقوانين في رصد صور الخطأ غير العمدي، ولكن قد يتعمد تداولها بدون ترخيص وهو على علم بذلك.[2]

نص المشرع التونسي في م52 على تجريم الاعتداء على السرية والخصوصية، بإفشاء معلومات عهد بها إلى مورد الخدمات الإلكترونية في إطار نشاطه، باستثناء تلك التي رخص له صاحب الشأن بنشرها بمقتضى شهادة كتابية أو إلكترونية.

يتحقق الركن المادي لهذه الجريمة بمجرد انتهاك سرية البيانات وخصوصيتها، دون اشتراط تحقق نتيجة إجرامية، أما الركن المعنوي فيتمثل في القصد الجنائي العام بعنصريه العلم والإرادة، ويمكن تصور ارتكاب الجريمة عن طريق الخطأ، إذا قام الجاني بالإفشاء في غير الحالات المحددة قانونا.

نص المشرع التونسي أيضا في م47 من قانون سنة 2000 سالف الذكر، على معاقبة كل من يصرح عمدا بمعطيات خاطئة لمورد خدمات التوثيق الإلكتروني، ولكافة الأطراف المطلوب منها الوثوق بإمضائه.

يتمثل الركن المادي لهذه الجريمة في إعطاء معطيات غير صحيحة لأحد الأطراف التي ذكرتهم المادة، ولم يشترط المشرع حصول نتيجة، أما الركن المعنوي فيتمثل في القصد الجنائي العام، ويتجلى ذلك بوضوح من لفظ "العمد" الوارد في نص المادة.[1]

---

[1] د. هدى حامد قشقوش، الحماية الجنائية للتجارة الإلكترونية عبر الانترنت، مرجع سابق، ص38-39.

[2] المرجع نفسه، ص40.

القانون التونسي نص على عقاب رادع لهذه الجريمة بالمادة 46 من قانون التجارة الالكترونية وهي عقوبة الحبس مدة تتراوح بين شهرين و3 سنوات وغرامة من 1000 إلى 10000 دينارا أو إحداهما.

يضاف إلى ذلك أن نص المادة 4 قد عاقب على عدم مراعاة قواعد كراسة الشروط المنصوص عليها بالقانون بالغرامة من 1000 إلى 10000 دينار، ثم لم يكتف القانون بذلك بل نص في المادة 44 منه على سحب الترخيص من مورد خدمات الوثائق الالكترونية وإيقاف نشاطه إذا أخل بواجباته التي نص عليها هذا القانون.

ويلاحظ أن المشرع التونسي بهذه النصوص قد فرض على مورد الخدمات التزامات محددة تحت طائلة العقوبة.

ثالثا: الحماية الجزائية للبيانات الشخصية في التشريع الجزائري

يجوز إعمال نصوص القسم السابع مكرر من ق ع المتعلق بحماية STAD، وهذه القواعد القانونية وخاصة المواد 394 مكرر، و394 مكرر1، و394 مكرر2 توفر حماية غير مباشرة للبيانات الاسمية، ولكنها لا تغطي جميع الحالات التي يمكن تصورها.

يرى البعض أنه يجوز إعمال نص م301 من ق ع،[2] لتوفير حماية جزائية للبيانات الاسمية، إلا أن جانبا من الفقه يرى أن محل الجريمتين مختلف، فجريمة إفشاء الأسرار تتطلب أن تكون المعلومات سرية، كما أن هنالك اختلافات أخرى بين الجريمتين ذكرت سابقا.[3] غير أن هذا لا يمنع من إعمال نص هذه المادة لتغطية بعض الحالات، وينبغي التدخل بنصوص خاصة لتدارك النقص.

أضاف المشرع الجزائري بموجب القانون رقم 06-23 المؤرخ في 2006/12/20،[4] إلى قانون العقوبات المواد 303 مكرر إلى 303 مكرر3، لحماية الحياة الخاصة للأفراد،[5] بحيث جرمت م303 مكرر[6] وعاقبت على أفعال المساس بحرمة الحياة الخاصة، بأي فعل من الأفعال التي ذكرتها المادة، وهي التقاط أو تسجيل أو نقل مكالمات أو أحاديث خاصة أو سرية، أو صورة شخص ،[7] في

---

[1] قشقوش، المرجع السابق، ص45.

أما عقوبة هذه الجريمة فهي الحبس من 6 أشهر إلى سنتين، والغرامة من 1.000 إلى 10.000 دينار أو إحدى هاتين العقوبتين.

[2] تنص م1/301 ق ع على: "يعاقب بالحبس من شهر إلى ستة أشهر وبغرامة من 500 إلى 5.000 دج الأطباء والجراحون والصيادلة والقابلات وجميع الأشخاص المؤتمنين بحكم الواقع أو المهنة أو الوظيفة الدائمة أو المؤقتة على أسرار أدلى بها إليهم وأفشوها في غير الحالات التي يوجب عليهم فيها القانون إفشاؤها ويصرح لهم بذلك".

[3] يراجع ما قيل حول إفشاء البيانات الاسمية في التشريع الفرنسي.

[4] ج ر 84، ص23.

[5] Tayeb Belloula, droit pénal des affaires et des sociétés commerciales, Berti éditions, Alger2011, p157.

[6] تنص م 303 مكرر على: "يعاقب بالحبس من ستة (6) أشهر إلى ثلاث (3) سنوات وبغرامة من 50.000 دج إلى 300.000 دج،كل من تعمد المساس بحرمة الحياة الخاصة للأشخاص، بأية تقنية كانت وذلك:

1-بالتقاط أو تسجيل أو نقل مكالمات أو أحاديث خاصة أو سرية، بغير إذن صاحبها أو رضاه.

2- بالتقاط أو تسجيل أو نقل صورة لشخص في مكان خاص، بغير إذن صاحبها أو رضاه.

يعاقب على الشروع في ارتكاب الجنحة المنصوص عليها في هذه المادة بالعقوبات ذاتها المقررة للجريمة التامة.

ويضع صفح الضحية حدا للمتابعة الجزائية.

[7] عبر المشرع عن الحديث الخاص بقوله"محادثات جرت في مكان خاص أو عن طريق التليفون". ومفهوم الحديث يعتبر أمرا سهلا إذ هو كل صوت له دلالة التعبير عن مجموعة من المعاني والأفكار المترابطة، فإذا كان هذا الصوت فاقد الدلالة على أي تعبير كالهمهمة والصيحات المتناثرة فلا يعد حديثا الصوت الذي وأن أعطى دلالة فلا يعطى دلالة التعبير عن مجموعة من المعاني والأفكار المترابطة كاللحن الموسيقي، أو التأوهات الجنسية إنما يستوي بعد ذلك أن تكون دلالة الصوت مفهومة للناس كافة أم لبعضهم فقط كالحديث الذي يتم بلغة أجنبية أو باستعمال الشفرة. وقد اعتبر المشرع هذا الحديث

مكان خاص بغير إذن صاحبها أو رضاه، وبأية تقنية كانت، فلا تهم الوسيلة المستعملة في ارتكاب النشاط الإجرامي لهذه الجريمة.

خاصا إذا جرى في مكان خاص أو عن طريق التليفون دون أن يكون مسموعا للكافة، كما لو جرى من أحد المقاهي أو المحال العامة أو بصوت عال في التليفون المحمول، وهذا معناه أن المشرع لا يأخذ بموضوع الحديث كمعيار لتحديد طبيعته، وإنما يتخذ من مكان حدوثه قرينة لا تقبل إثبات العكس على طبيعته. فيكون الحديث خاصا إذا جرى في مكان خاص أو في التليفون أي باستخدام تقنية التليفون السلكي أو المحمول ولو تناول موضوعا عاما لا علاقة له بالحياة الخاصة لقائله ويعتبر الحديث على العكس عاما إذا جرى في مكان عام ولو تناول أخص شئون قائله وأسراره وهو معيار يتسم بالوضوح وله فوق ذلك ما يبرره، فالحديث الذي يلقى به الشخص في مكان عام يكون متاحا للكل سماعة ولا يمثل تسجيله أو نقله أي عدوان على الحياة الخاصة لقائله ولو تناول أخص أسراره، لأنه لا يجوز للشخص أن يفرط في إسراره ثم يطلب حماية القانون الجنائي، أما الحديث الذي يجريه صاحبه في مكان خاص أو عن طريق التليفون دون أن يكون مسموعا للكافة بوضوح كما يجري أحيانا عند الحديث في التليفون المحمول. فهو حديث يتم–ولو كان في موضوع عام– مع من يزيد ومن فيهم يثق وقد لا يكون محتاطا لخطورة الموضوع أو لسريته أو لدقته.

ويكون الحديث قد جرى في مكان خاص وبالتالي خاصا إذ جرى عن طريق التليفون أو في مكان مغلق لا يمكن دخوله إلا لأشخاص يرتبطون مع بعضهم بصلة خاصة ولا يمكن للخارج عنه أن يشاهد ما يجري بداخله أو أن يسمعه. وعلى هذا الأساس فإن الحديث يكون علما إذا جرى في مكان مغلق يجوز لمن يرغب من الكافة دخوله، أو في مكان مفتوح متاح لكل من يرغب أن يستمع لما يدور فيه، أو في مكان مغلق لكن يمكن للخارج عنه أن يشاهد ما يجري بداخله وأن يسمعه بسبب وجود آلات لتكبير الصوت مثلا.

وهكذا فالحديث الخاص الذي يحميه القانون هو الحديث الذي يجري إما في مكان خاص وإما بطريق التليفون (فيما عدا الحديث الذي يجري بالتليفون السلكي من مكان عام وبصوت عال دون تحوط كما لو أجراه في مقهى أو في محل عام، أو بطريق التليفون المحمول إذا جرت بصوت عال ومسموع للكافة دون استراق السمع) أياما كانت طبيعته وعلى نحو لا يقبل إثبات العكس. وقد وفر القانون لهذا الحديث الحماية سواء من استراق السمع أو من تسجيل الحديث أو نقله، والأمور الثلاثة متعادلة بحيث يكفي تحقق أحدهما لقيام الجريمة إذا تكاملت بقية عناصرها.

ويقصد باستراق السمع: التنصت على الحديث أو الاستماع إليه خلسة، وهو فعل يتم باستخدام الإذن وحدها دون إلى الاستعانة بأية أداة أو جهاز، وعلى هذا يرتكب الجريمة من يتنصت بأذنيه على حديث خاص، سواء حفظه في ذاكرته ثم نقله لآخرين أم لم ينقله.

ويقصد بتسجيل الحديث: حفظه على الأشرطة المخصصة لذلك لإعادة الاستماع إليه من بعد، أما نقل الحديث فيقصد به استراق السمع عن طريق جهاز لإرساله من المكان الذي يقال فيه إلى مكان آخر بواسطة أجهزة الاستماع أو ميكروفونات الإرسال، وفي هاتين الصورتين– التسجيل والنقل– يتم الحصول على الحديث بالاستعانة بجهاز وبالنظر إلى أن التطور العلمي الحديث قد أخرج في هذا المجال صنوفا لا تحصى من الأجهزة سواء للتسجيل أو الإرسال فقد تحوط المشرع لتجريم كافة ما يمكن أن يصل إليه العلم في هذا المجال بعبارة بجهاز من الأجهزة أياما كان نوعه.

ويشترط أخيرا أن يكون استراق السمع أو تسجيل الحديث الخاص أو نقله قد تم بغير رضاء المجني عليه: وقد سبق لنا أن حددنا مفهوم الرضا بأنه الموافقة على سماع الحديث أو تسجيله أو نقله، هذه الموافقة يلزم أن تكون حرة لكن يستوي أن تكون صريحة أو ضمنية (كما لو كان يتحدث بصوت عال ومسموع للكافة من تليفون أرضي في مقهى أو محل عام أو لمن يتحدث بصوت عال ومسموع للكافة بلا مشقة في تليفونه المحمول على المقهى أو الطريق أو في محل عام). وقد اعتبر المشرع المصري أن سماع الحديث أو تسجيله أو نقله على مرأى أو مسمع من الحاضرين في الاجتماع رضاء مفترضا من جانبهم بسماع الحديث أو تسجيله أو نقله.

التقاط الصورة يعني تثبيتها على مادة حساسة(النيجاتيف). وتقع الجريمة بمجرد التقاط الصورة أي بمجرد تثبيتها أما إظهارها على المادة المخصصة لذلك فليس شرطا لتمام الجريمة وعليه فإن إضفاء بعض التشويهات على النيجاتيف لتعطيها مظهرا كاريكاتوريا أو مغايرا لا يؤثر في قيام الجريمة. أما النقل فيعني إرسال الصورة مباشرة إلى مكان آخر عاما كان أو خاصا بحيث يتمكن الغير من الاطلاع عليه على نحو ما يحدث بالنسبة للإرسال التليفزيوني.

ويشترط أخيرا أن يكون التقاط الصورة الخاصة أو نقلها قد حدث بغير رضاء المجني عليه، أي دون موافقته الصريحة أو الضمنية مع ملاحظة أن المشرع قد افترض رضاء صاحب الصورة إذا التقطت له أو نقلت على مرأى ومسمع من الحاضرين في الاجتماع رضاء مفترضا من جانبهم بسماع الحديث أو تسجيله أو نقله. يراجع: د. محمد زكي أبو عامر، الحماية الجنائية للحرية الشخصية، دار الجامعة الجديدة، الإسكندرية، مصر 2011، ص ص85–88.

حسب محكمة نقض باريس فإنه يقصد بالمكان الخاص:"المكان الذي لا يجوز دخوله إلا بإذن شاغليه".[1]

كما أن م303 مكرر1،[2] عاقبت وجرمت على التعامل بالأشياء المتحصل عليها من الجرائم المذكورة في المادة السابقة بالعقوبة ذاتها المقررة في م303 مكرر.

الملاحظ أن المشرع الجزائري قد أخذ هاتين المادتين عن المشرع الفرنسي(م226-1، 226-2 ق ع ف).[3]

السؤال الذي يثور: هل يجوز إعمال نص هاتين المادتين لحماية البيانات الاسمية في مجال التجارة الالكترونية؟

إن هاتين المادتين لم توضعا أصلا لحماية البيانات الاسمية في التجارة الالكترونية سواء من قبل المشرع الفرنسي أو الجزائري، ولذلك يتبادر في الذهن للوهلة الأولى أنه من غير المتصور إعمالهما، ولكن رغم ذلك هما توفران حماية غير مباشرة للحياة الشخصية للمستهلك الإلكتروني في الفرض الذي يتتبع أحدهم هذا المستهلك عبر الانترنت ويقوم بالتقاط أو تسجيل أو نقل مكالمات أو أحاديث خاصة أو سرية، أو صورة الشخص عن بعد (الانترنت) عند اتصاله بالتاجر عبر هذه الوسيلة.

المطلب لثاني: المسؤولية الجزائية لمقدمي الخدمات الوسيطة عبر الانترنت.

حتى يتمكن مستخدمو الإنترنت من الدخول إلى الشبكة، والإبحار فيها بحرية، والوصول إلى ما يصبون إليه من معلومات أو بثها، والدخول إلى المواقع التجارية، لا بد من وجود عدة أشخاص، يطلق عليهم عادة مصطلح "مقدمي خدمات الإنترنت"، أو "الوسطاء في خدمات الإنترنت"، مهمتهم إيواء المعلومات، بثها، وعرضها، هذا التنوع في أدوارهم والتعدد في أنشطتهم وضع بهدف تسهيل تتبع النشاط المعلوماتي غير المشروع وكشفه، إلا أن تحقيق ذلك يبقى رهن وجود

[1] Cass. Crim,28/11/2006, voir Béatrice Clément et autre, op cit, p117.

[2]تنص هذه المادة على: "يعاقب بالعقوبات المنصوص عليها في المادة السابقة كل من احتفظ أو وضع أو سمح بأن توضع في متناول الجمهور أو الغير، أو استخدم بأية وسيلة كانت، التسجيلات أو الصور أو الوثائق المتحصل عليها بواسطة أحد الأفعال المنصوص في م303مكررمن هذا القانون".

[3] Béatrice Clément et autre, op cit, p116-120.

ضوابط قانونية تحدد حقوق أطراف النشاط الإلكتروني، والتزاماتهم في مواجهة بعضهم بعضا من جهة، وفي مواجهة المجتمع الذي يعيشون فيه من جهة أخرى، لذا بدت الحاجة ماسة لإيجاد تنظيم تشريعي متكامل يحدد المركز القانوني لمقدمي خدمات الإنترنت، ويبين في الوقت نفسه مسؤولية كل منهم عما يرتكب من مخالفات عبر الشبكة، الأمر الذي لا يمكن تحقيقه إلا بتضافر جهود المشرعين على الصعيدين الوطني والدولي.

هذه الحقيقة كانت نواة عمل البرلمان الأوروبي الذي تبنى بالإجماع في 08 جوان عام 2000 التوجيه رقم 2000/31، والمتعلق "ببعض الأوجه القانونية لخدمات شركات المعلومات، وبصفة خاصة التجارة الإلكترونية في السوق الداخلي"، ويعتبر النواة الأولى والتشريع الإطار الذي أخذ في الحسبان أنواع الأنشطة المرتبطة بالانترنت، وكذا مستخدميها،[1] وتم تخصيص القسم الرابع منه لتنظيم المركز القانوني للوسطاء في خدمات الإنترنت، وذلك على غرار القانون الأمريكي الصادر عام 1998 للحد من الاعتداءات على حقوق الملكية الفكرية في نطاق الإنترنت والمسمى بـ Digital Millenium Copyright Act (DMCA)، والذي خصص الباب الثاني منه لتحديد مسؤولية مقدمي خدمات الإنترنت عن التعدي على هذه الحقوق،[2] علما أن المشرع الأمريكي كان قد أصدر من قبل قانون عرف ب (CDA)،[3] ولكن اعتراه بعض العوار القانوني وبعض النقص، فحل محله (DMCA) الذي لم يكن يهدف سوى إلى توجيه أسئلة بخصوص الانترنت لإيجاد أجوبة لها، وقد عكس مختلف المبادئ المتبناة في مجال حقوق التأليف، ووفق هذا المعنى عرفت مسؤولية وسطاء شركات المعلومة في مجال التقليد. [4]

وجاءت م22 من التوجيه الأوروبي لتلزم الدول الأعضاء في الاتحاد الأوروبي على نقل أحكامه إلى تشريعاتهم الداخلية بحلول عام 2002، والتزاما منها بذلك قدمت الحكومة الفرنسية عام 2001، كمحاولة أولى، مشروع قانون حول "شركات المعلوماتية"، والذي حددت في قسم منه المركز القانوني لمزودي خدمات الإنترنت، إلا أن هذا المشروع ألغي، فتقدمت الحكومة الفرنسية من جديد عام 2003 بمشروع قانون حول "الثقة في الاقتصاد الرقمي"، والذي تم الموافقة عليه من قبل المشرع

[1] Régis Buchillet, la responsabilité des prestataires techniques de l'internet, DEA en droit de l'économie, mention droit international, université de Bourgogne, France 2001/2002, p5.

[2] محمد حسين منصور، المرجع السابق، ص159.

[3] Communication Decency Act.

[4] Régis Buchillet, op cit, p25.

الفرنسي في 21 جوان 2004، واعتبارا من هذا التاريخ أصبح لمقدمي خدمات الإنترنت في فرنسا نظامهم القانوني الخاص.[1]

وكان الهدف من هذا القانون هو إخراج "متعهدي تقديم خدمات الانترنت" من الإطار التقليدي للمسؤولية عن طريق الخطأ أو عن طريق الإهمال، وإيجاد نظام مسؤولية خاص يتوافق وطبيعة عملهم.[2]

وبالنسبة للدول العربية فإن أغلب تشريعاتها لم تضع نظاما خاصا بهذه الفئة، والسؤال الهام الذي يثور هنا هو: ما جدوى إعمال القواعد العامة لتحديد المركز القانوني لمقدمي الخدمات، وبالنتيجة مدى ملاءمة الحلول المستقاة في هذا الصدد؟

إن اللجوء إلى القواعد العامة لتحديد التزامات مقدمي خدمات الإنترنت ومسؤولياتهم أمر سينتابه القصور، وذلك لسببين: أولهما، حداثة المشاكل التي يُثيرها هذا المجال، وبالتالي عجز هذه القواعد عن المواكبة الدقيقة والفعالة للتطور التكنولوجي الحاصل فيه، وثانيهما، خصوصية تقديم خدمات الوساطة على الإنترنت، والتي تحتاج لبيئة تشريعية خاصة ومتوازنة، إن هذه الأسباب، كانت الدافع الرئيس للقضاء في فرنسا وأمريكا وغيرهما من الدول لهجر تطبيق القواعد العامة على خدمات الوساطة على الإنترنت، ولابتكار ضوابط قانونية خاصة ذات حلول ملائمة، وقد استمر قضاء هذه الدول على هذا النهج إلى أن تبني مشرعوهم قواعد خاصة ومتوازنة أرسوا فيها النظام القانوني لمقدمي خدمات الإنترنت، من حيث تحديد طبيعة عملهم والتزاماتهم، ومسؤولية كل منهم في مواجهة السلسلة المعلوماتية المتواصلة عبر الشبكة.[3]

وتأسيسا على ما تقدم، يتم دراسة هذا الموضوع من خلال ثلاثة فروع، يتناول الفرع الأول الطبيعة القانونية لخدمات الإنترنت وصفة مقدميها، والفرع الثاني يتصدى لتحديد التزامات مقدمي خدمات الإنترنت، ويعالج الفرع الثالث مسؤولية مقدمي خدمات الإنترنت عما يحدث من مخالفات عبر الشبكة.

---

[1] Christiane Féral-Schul,cyberdroit,le droit à l'épreuve de l'internet. Dalloz, Paris 2008,p701.

[2] Eric Barbry, le droit de l'internet est devenu au fil des années un droit spécial? Gazette du palais5, septembre octobre 2010, p3168.

[3] محمد حسين منصور، المرجع السابق، ص161.

الفرع الأول: الطبيعة القانونية لخدمات الإنترنت وصفة مقدميها.

إن حصول الجمهور على المعلومات، أو بثها عبر شبكة الإنترنت، لا يمكن أن يتم دون الاستعانة بخدمات القائمين عليها، وهم، كما عرفتهم المادتان: 14 من التوجيه الأُوروبي حول "التجارة الإلكترونية" و6-2/1 من القانون الفرنسي حول "الثقة في الاقتصاد الرقمي": "الأشخاص الطبيعيون أو المعنويون الذين يتولون، ولو بالمجان، تخزين البيانات والسجلات المعلوماتية لعملائهم، ويضعون تحت تصرفهم الوسائل التقنية والمعلوماتية التي تُمكنهم من الوصول إلى هذا المخزون الإلكتروني على مدار الساعة".[1]

من خلال هذا التعريف، يتبين تنوع الخدمات التي يقدمها القائمون على إدارة شبكة الإنترنت، وبالنتيجة اختلاف طبيعتها القانونية وتعدد صفة مقدميها، فمن هذه الخدمات ما هو مخصص لتقديم المضمون المعلوماتي لجمهور مستخدمي الشبكة، ومنها ما يهدف إلى توفير الوسائل الفنية اللازمة لربط شبكات الاتصال، وتمكين العملاء من الوصول إلى المادة المعلوماتية المبثوثة عبر الإنترنت.

أولا : خدمات الإيواء.

إن مصطلح إيواء (hébergement)، بمعناه الإلكتروني الواسع، يشمل وضع الوسائل التقنية المعلوماتية بمقابل أو بالمجان تحت تصرف العملاء، ليتمكنوا من الدخول إلى شبكة الإنترنت في أية لحظة، بُغية بث مضمون معلوماتي معين: (نصوص، أو صور، أو أصوات...) للجمهور، ويتولى هذه المهمة متعهد للإيواء (fournisseur d'hébergement) يعمل على تخزين البيانات والمعلومات التي يبثها أصحاب المواقع الإلكترونية على حاسباتهم الآلية المرتبطة على الدوام بشبكة الإنترنت، بحيث يتمكن أصحاب هذه المواقع من إطلاع الجمهور على مضمونها المعلوماتي على مدار الساعة.

إن خدمة الإيواء، كما عرفتها المادة 14 من التوجيه الأوروبي حول "التجارة الإلكترونية" والمادة 6-2/1 من القانون الفرنسي حول "الثقة في الاقتصاد الرقمي": عبارة عن نشاط يُمارسه شخص طبيعي أو معنوي، يهدف إلى تخزين مواقع إلكترونية وصفحات ويب على حاسباتهم الآلية الخادمة

[1] عبد الفتاح بيومي حجازي، المرجع السابق، ص123.

بشكل مباشر ودائم مقابل أجر أو بالمجان، ويضع، من خلاله، تحت تصرف عملائه الوسائل التقنية والمعلوماتية التي تُمكنهم في أي وقت من بث ما يريدون على شبكة الإنترنت، من نصوص، وصور، وأصوات، وتنظيم المؤتمرات والحلقات النقاشية وإنشاء روابط معلوماتية مع المواقع الإلكترونية الأخرى... [1]

من الوسائل التي يقدمها متعهد الإيواء لعملائه تخصيص مساحة قرص أو شريط مرور لبث المعلومات التي يرغبون بنشرها على شبكة الإنترنت، وتزويد العميل بحساب خاص يتضمن مفتاح دخول (code d'accès) للتعريف به، وتزويده ببرنامج خاص يمكنه من الاتصال بمتعهد الإيواء، وإضافة، حذف، أو تغيير ما يريد من معلومات.

إن الإيواء أو التخزين المباشر والدائم للمواقع الإلكترونية ولصفحات الويب على الحاسبات الآلية لمتعهد الإيواء، والمرتبطة على الدوام بشبكة الإنترنت، هو الذي يميز هذا الأخير عن الناقل الفني البسيط (cashing) الذي يتولى، في سبيل تسريع عملية اتصال الجمهور بالشبكة، الاحتفاظ أوتوماتيكيا بنسخة مؤقتة عن كل صفحة ويب ينقلها إلى طالبيها من المستخدمين. فالدور الهام الذي يضطلع به متعهدو الإيواء في إدارة الإنترنت يفرض، حتما، على كل من يرغب بالبث المباشر والدائم لمضمون معلوماتي ما على الشبكة، اللجوء إلى واحد منهم للاستعانة بخدماته؛ فهم كأصحاب أجهزة تخزين مركزية، يشكلون عنصرا رئيسا من العناصر المكونة لشبكة الإنترنت، وتربطهم بعملائهم، من أصحاب المواقع الإلكترونية، رابطة تعاقدية يتم تنظيمها من خلال عقد خاص يُسمى عقد الإيواء، وعادة ما يتم توقيعه إلكترونيا من قبل الطرفين.

ويلعب هذا العقد دورا جوهريا في التعرف على شخصية طالب الخدمة، وبإحاطته علما بشروط استعمالها، وبإعلامه بوجوب عدم تجاوز الإطار الصحيح والمشروع لاستخدام الوسائل التقنية والمعلوماتية المخصصة له، وذلك تفاديا لإلحاق الضرر بمتعهد الإيواء وبالغير، كذلك يعد عقد الإيواء مصدرا مهما لتحديد التزامات مقدم الخدمة؛ فبالإضافة لالتزام متعهد الإيواء الأصلي، المتمثل بتقديم الوسائل التقنية والمعلوماتية لتمكين العملاء من بث ما يرغبون من معلومات، يلتزم متعهد الإيواء

[1] Les personnes physiques ou morales qui assurent, même à titre gratuit, pour mise à disposition du public par des services de communication au public en ligne, le stockage de signaux, d'écrits, d'images, de sons ou de messages de toute nature fournis par des destinataires de ces services...
il a été jugé que l'organisateur d'un forum de discussion est un hébergeur : TG I Lyon, 21/07/2005, voir : Jaque Larrieu ; op cit, p160.

أحيانا، ببعض الخدمات الإضافية، كالتزامه بتقديم المساعدة الفنية للعملاء، أو مساعدتهم على إنشاء مواقع إلكترونية خاصة بهم، أو تقديم خدمات البريد الإلكتروني وأنظمة البحث الآلي... وهذا النوع من الالتزامات يثير إشكاليات تقنية أكثر منها قانونية، الأمر الذي يؤدي أحيانا، إلى صعوبة الدخول للمواقع الإلكترونية المطلوبة، إما بسبب التزاحم الشديد على الدخول إلى الشبكة، أو بسبب الانقطاع المفاجئ للاتصال بها، أو لغيره من الأسباب، وهنا تؤسس مسؤولية مقدم الخدمة على القواعد الخاصة بتنفيذ الالتزام العقدي.[1]

وفي إطار الالتزام العقدي، ومن أجل تحديد الطبيعة القانونية للخدمة التي يقدمها متعهد الإيواء، يجب التمييز بين من يزود خدمة الإيواء بمقابل ومن يزودها بالمجان؛ فإيواء صاحب الموقع الإلكتروني للمادة المعلوماتية على الحاسبات الآلية لمتعهد الإيواء مقابل أجر، يمكنه من الاستفادة من الوسائل التقنية والمعلوماتية لمقدم الخدمة، ومن استخدام مساحة معينة من قرصه الصلب، بحيث يبقى على اتصال مباشر ودائم بشبكة الإنترنت، ويتم تقدير الأجر حسب الاتفاق، وبشكل يتناسب مع حجم المعلومات المراد بثها، ومدة هذا البث، فتقديم خدمة الإيواء بمقابل هو بمنزلة تأجير لجزء من القرص الصلب أو لمكان على الشبكة تابع لمتعهد الإيواء، أما الإيواء بالمجان فيتمثل بإعارة جزء من القرص الصلب، أو مكان على الشبكة تابع لمتعهد الإيواء، وتكييف خدمة الإيواء قانونا على أنها إجارة أو إعارة، بحسب وجود المقابل من عدمه أمر يتفق وأحكام القانون.

وعلى ذلك، يتوجب على صاحب الموقع الإلكتروني، مستأجرا كان أم مستعيرا، استعمال المساحة المخصصة له استعمالا مشروعا متفقا مع بنود العقد الذي يربطه بمتعهد الإيواء من ناحية، ومع القواعد القانونية الواجبة التطبيق من ناحية أخرى، وبالمقابل، على متعهد الإيواء مؤجرا كان أم معيرا تأمين مساحة من قرصه الصلب المرتبط على الدوام بشبكة الإنترنت لصالح صاحب الموقع الإلكتروني، وتمكينه بشكل مباشر ودائم من بث ما يرغب به من معلومات عبر الشبكة، وذلك وفقا لما تم الاتفاق عليه في عقد الإيواء، وإيواء المعلومات على شبكة الإنترنت يختلف عن توريدها، ذلك أن توريد المعلومات عبر الشبكة يعني نشرها وإطلاع الجمهور على مضمونها، وهو ما يتعدى حدود الدور التقليدي لمتعهد الإيواء الذي يقتصر على تخزينها.[2]

---

[1] بيومي حجازي، المرجع السابق، ص141.

[2] محمد حسين منصور، المرجع السابق، ص 171.

ثانيا: خدمات توريد المعلومات

توريد المعلومات هو نشرها، أي إطلاع الجمهور على مضمونها، بحيث تكون مقروءة لهم، أو مرئية، أو مسموعة، وتعتبر خدمة توريد المعلومات عبر الانترنت "وسيلة اتصال علنية" هدفها وضع مادة معلوماتية معينة (نصوص، رسائل، صور، أصوات...) تحت تصرف مستخدمي الشبكة.

يُقصد بتوريد المعلومات عبر الشبكة، تحميل المساحة المستأجرة، أو المعارة من القرص الصلب، أو من أجهزة التخزين المركزية التابعة لمتعهد الإيواء بالبيانات والمعلومات التي يقوم مورد المعلومات (fournisseur du contenu)، باعتباره صاحب وسيلة اتصال علنية، بجمعها أو تأليفها حول موضوع معين؛ فمورد المعلومات قد يكون صاحب المادة المعلوماتية، أي مؤلفها، كما يُمكن أن يقتصر دوره على جمعها، أي التوسط ما بين مؤلف المادة ومستخدمي الشبكة الراغبين في الإطلاع على مضمونها، فيتخذ في الحالة الأولى، في آن واحد، صفة مؤلف المادة المعلوماتية والناشر لها من خلال خدمة التوريد، ويتخذ في الحالة الثانية صفة الناشر فقط، وبهذه الصفة الأخيرة يقوم مورد المعلومات بنشرها على شبكة الإنترنت بناء على عقد نشر يربطه بصاحب المادة المعلوماتية، ومن هنا، فإن مورد المعلومات، سواء أكان شخصا طبيعيا أم معنويا، هو صاحب السلطة الحقيقية في مراقبة المضمون المعلوماتي الإلكتروني؛ لأنه هو من يقوم بتأليفه أو جمعه، وبالتالي فإنه يملك توريده لمستخدمي الشبكة أو الامتناع عن ذلك، وهذا الدور كان وراء تشبيهه بمورد المضمون المعلوماتي التقليدي، مثل مدير النشر ورئيس التحرير في الصحافة المكتوبة، ووكالات الأنباء، ووسائل الاتصال المرئية والمسموعة، والذي يقوم بمراقبة المادة المحررة في وسيلة إعلامه بشكل يضمن تقديم المادة المعلوماتية الحقيقية والمشروعة.

وبذلك، فإن مورد المعلومات يتميز عن متعهد الإيواء، من حيث أن هذا الأخير لا يقوم بتأليف أو جمع المضمون المعلوماتي الإلكتروني، وإنما يعمل فقط على تخزينه على أجهزته بناء على اتفاقه مع مورد المعلومات ليتسنى للجمهور الاطلاع عليه على مدار الساعة، فخدمة التوريد هي خدمة نشر، والمورد هو الناشر، أما خدمة الإيواء فهي خدمة تأجير أو إعارة مكان على الشبكة، ومتعهد الإيواء هو المؤجر للمكان أو المعير له. وبالرغم من هذا الاختلاف، إلا أنهما يلتقيان في المساهمة بتقديم الخدمة المعلوماتية عبر الإنترنت، فالبيانات والمعلومات لا يمكن أن تُبث عبر الشبكة

دون تدخلهما، ولا يمكن، في الوقت ذاته، أن تصل إلى الجمهور دون وجود الوسائل الفنية اللازمة للربط المادي بين شبكات الاتصال عن بُعد والحاسبات الآلية للمستخدمين.[1]

ثالثا: خدمات النقل المادي للمعلومات.

إن اطلاع مستخدمي الإنترنت على المادة المعلوماتية المنشورة عبر الشبكة يقتضي، عمليا، ربط حاسباتهم الآلية بالمواقع الإلكترونية، وهو ما يحتاج إلى إجراء ربط مادي وفني بين شبكات الاتصال عن بعد، وغالبا ما تتولى هذه العملية الهيئات العامة للاتصال، (فرانس تيليكوم في فرنسا) والتي تلتزم، كناقل مادي للبيانات والمعلومات، وتنفيذا لعقد نقل المعلومات الذي يربطها بباقي مقدمي خدمات الإنترنت، بتقديم الوسائل والأجهزة الفنية اللازمة لإجراء عملية النقل المادي للمادة المعلوماتية، وذلك من خلال الربط المشترك بين مختلف شبكات الاتصال عن بعد.

فتقديم خدمة نقل المعلومات يتم بموجب عقد نقل، الخدمة هي خدمة نقل، ومقدمها هو الناقل (transmetteur)، وبهذا الوصف يمكن تشبيه ناقل المعلومات، عبر شبكة الإنترنت، بساعي البريد، فكلاهما تنحصر مهمته في تأمين النقل المادي للمعلومات بين مختلف الأطراف من مرسلين ومرسل إليهم، وهذا ما يميزه عن غيره من مقدمي خدمات الإنترنت، كمتعهد الإيواء ومورد المعلومات، فهو لا يتولى عملية التخزين المباشر والدائم للمادة المعلوماتية ولا يقوم بجمعها أو تأليفها، وبالنتيجة فإنه ليس بصاحب سلطة حقيقية عليها، وإنما جل عمله ينصب على عملية نقلها ماديا من وحدة إلى أخرى، دون أن يكون مكلفا بمراقبتها أو بمعرفة مضمونها.

رابعا: خدمات الوصول.

تتمثل عملية تقديم خدمات الدخول أو الوصول إلى الإنترنت في تزويد متعهد الوصول أو الولوج (fournisseur d'accès)[2] مستخدمي الشبكة المشتركين معه (les abonnés) بموجب عقد "تقديم خدمات الدخول" بالوسائل والأجهزة الفنية اللازمة لدخولهم إلى شبكة الانترنت، والتي تمكنهم من الإبحار فيها بحرية، ومن الوصول إلى المواقع الإلكترونية التي يرغبون الاطلاع على مضمونها، فالنشاط المحوري لمتعهد الوصول هو تقديم خدمة الدخول إلى شبكة

[1] محمد حسين منصور، المرجع السابق، ص 176.

[2] Les FAI sont Les personnes dont l'activité est d'offrir un accès à des services de communication au public en ligne.

الإنترنت للمشتركين معه من جمهور المستخدمين، الأمر الذي يتطلب تزويدهم بمفتاح دخول، وبكلمة سر، وببريد إلكتروني بغية استقبال وإرسال الرسائل الخاصة بهم...

بالإضافة إلى هذا النشاط الرئيس، يقترح متعهد الوصول على مشتركيه خدمات إضافية أخرى، كاقتراحه لمضمون معلوماتي معين يتم بثه عبر الشبكة أو التعهد بإيوائه، أو فتح حلقات للنقاش، أو نشر بيانات ومعلومات معينة على صفحات الويب التابعة له، أو حتى تخزين صفحات الويب التي يُطلع عليها مشتركيه بصورة مؤقتة من أجل تسريع عملية وصولهم إليها عند طلبها مرة أُخرى... ويتم الاستفادة من هذه الخدمات عن طريق الدخول إلى صفحة الويب الرئيسة للموقع الإلكتروني الخاص بمتعهد الوصول، غير أنه لا يقدمها هنا بصفته متعهد وصول فقط وإنما بوصفه متعهد إيواء، وبالتالي، يخضع فيما يخص الخدمات الإضافية، للأحكام الخاصة بهذا المتعهد.

وعند الرجوع إلى طبيعة النشاط أو العمل الرئيس الذي يمارسه متعهد الوصول، كعامل فني للاتصالات عن بعد، فإن المادة 32-15 من قانون البريد والاتصالات عن بعد تعرفه بهذه الصفة، على أساس أنه: "كل شخص طبيعي أو معنوي يستغل شبكة الاتصالات عن بعد، والمفتوحة للجمهور، أو يُورد لهم خدمة الاتصالات عن بعد"، ولغايات تطبيق هذا النص، أوضحت المادة 32-2 من القانون نفسه أن المقصود بشبكة الاتصالات عن بُعد هو "كل تجهيز أو مجموعة التجهيزات التي تؤمن نقل وتوجيه إشارات الاتصالات عن بعد، وتُمكن من تبادل المعلومات، ومن إدارتها بين نقاط النهاية لهذه الشبكة".

من خلال الربط بين التعريف الوارد في نص هذه المادة وتعريف متعهد الوصول الذي ورد في نص المادة 32-15 السابقة الذكر، عدت الهيئة الفرنسية لتنظيم قطاع الاتصالات عن بعد في تقرير لها صدر في نهاية عام 1998 أن الوصف الوارد في نص المادة 32-2 يتطابق تماما مع طبيعة العمل الأصلي الذي يقوم به متعهد الوصول، والذي يلتزم من خلاله، استنادا إلى عقد "تقديم خدمات الدخول" الذي يربطه بعملائه، بإيصالهم إلى شبكة الإنترنت وبتأمين التجهيزات اللازمة لنقل إشارات الاتصالات عن بُعد وتوجيهها، ولتبادل المعلومات وإدارتها لقاء مقابل، كل ذلك شريطة أن يتعهد العملاء باحترام شروط الاستفادة من هذه الخدمة.

وعليه، فإن عقد "تقديم خدمات الدخول" هو عقد ملزم لجانبين، محله بالنسبة لمتعهد الوصول تزويد العميل بالوسائل الفنية والبرمجيات التي تمكنه من الالتحاق بشبكة الإنترنت، وبالنسبة للمشترك دفع قيمة الاشتراك حسب ما اتفق عليه، ومن هنا، فإن الخدمة التي يقدمها متعهد الوصول هي أشبه بمقاولة، وبالتالي، فإن "عقد تقديم خدمات الدخول" هو عقد مقاولة يلتزم بمقتضاه متعهد الوصول (المقاول) بتقديم خدمة الدخول، وبعمل ما يلزم لتحقيق هذه الغاية لقاء مقابل يلتزم طالب الخدمة بدفعه، ويتطابق هذا التكييف مع تعريف عقد المقاولة الوارد في م1710 من القانون المدني الفرنسي، إذْ عرفته على أنه عقد يتعهد بموجبه أحد الطرفين بأن يضع شيئا، أو يؤدي عملا لقاء بدل يتعهد به الطرف الآخر.[1]

يشترك العديد من الأشخاص في إدارة شبكة الانترنت، وتختلف الطبيعة القانونية للخدمات التي يقدمونها، وكذلك تتعدد صفاتهم، الأمر الذي يؤدي حتما إلى تنوع التزاماتهم.

الفرع الثاني: التزامات مقدمي خدمات الإنترنت.

يتضح جليا مما تقدم، تنوع مهام أشخاص القائمين على خدمات الإنترنت، وتعدد أدوارهم المتبادلة، إذ من الممكن للشخص الواحد أن يقوم في الوقت نفسه بمهمة أو أكثر. ويثور التساؤل حول كيفية تحديد التزامات كل شخص من أشخاص القائمين على خدمات الإنترنت، فمن هؤلاء الأشخاص من يتسم عمله على الشبكة بالطابع المعلوماتي، ومنهم من يغلب على عمله الطابع الفني، الأمر الذي يستدعي تحديد التزامات كل من مقدمي الخدمة المعلوماتية، ومقدمي الخدمة الفنية.[2]

أولا: التزامات مقدمي الخدمة المعلوماتية.

إن طبيعة الخدمة التي يقدمها متعهد الإيواء تجعله، حتما الأقرب والأقدر على معرفة مضمون أي نشاط معلوماتي متداول عبر شبكة الإنترنت، وإذا ما ثبتت عدم مشروعية المضمون محل الإيواء فإن ذلك سيثير عددا من الإشكالات القانونية على صعيدين مختلفين: الأول، يتعلق بمدى التزام متعهد الإيواء برقابة المضمون المعلوماتي المتداول عبر شبكة الإنترنت، والثاني، يتمثل في الالتزامات التي تقع على عاتق متعهد الإيواء في حال علمه بتداول مضمون معلوماتي غير مشروع عبر

[1] بيومي حجازي، المرجع السابق، ص136.

[2] أحمد فرح، النظام القانوني لمقدمي خدمات الانترنت، مجلة المنارة، المجلد 13، العدد9، الكويت 2007، ص330.

هذه الشبكة، وأمام هذه الإشكالات، وفي ظل غياب نص تشريعي خاص يعالجها، فرض القضاء الفرنسي حدا معقولا من الالتزامات على متعهدي الإيواء، فما كان من المشرع الفرنسي إلا أن استجاب لهذا القضاء و قنن هذه الالتزامات أسوة بالمشرع الأوروبي.[1]

لم يكن من السهل في البداية على القضاء الفرنسي، وأثناء نظره الدعاوي المرفوعة ضد متعهدي الإيواء، تحديد نطاق الالتزامات ومضمونها التي تقع على عاتقهم، فحاول جاهدا التغلب على الصعوبات التي واجهته كي لا تكون الإنترنت منطقة بلا قانون، ونظرا لطبيعة الخدمة التي يقدمها متعهدو الإيواء، وفي ظل غياب نصوص قانونية خاصة، أبدى القضاء الفرنسي قدرا من التساهل في نوعية الالتزامات الملقاة على عاتقهم، فلم يفرض عليهم التزاما عاما بممارسة الرقابة الدقيقة على محتويات المواقع الالكترونية التي يأوونها، ولم يكلفهم بالبحث النشيط عن المضمون المعلوماتي الإلكتروني غير المشروع، ولكنه بالمقابل ألزمهم بأخذ الحيطة والحذر، وأقام مسؤولياتهم عند التقصير، وقد استند القضاء في ذلك على القواعد العامة في المسؤولية، وبالأخص نص المادتين: 1382 و1383 من القانون المدني الفرنسي اللتين تُلزمان صاحب الفعل الضار الذي أدى بخطئه، أو بإهماله، أو بتقصيره إلى الإضرار بالغير بضمان هذا الضرر.[2]

---

[1] المرجع نفسه، ص332.

[2] وتطبيقا لذلك، وبمناسبة الاعتداء على الحق في الصورة من قِبل متعهد الإيواء Altern.org، أقامت عارضة الأزياء الفرنسية Estelle Hallyday دعوى قضائية أمام محكمة باريس الابتدائية ضد V. Lacambre مؤسس وصاحب الموقع Altern.org تُطالبه فيها بالتعويض عن الأضرار التي سببها لها نتيجة لإيوائه موقعا إلكترونيا نشر عليه تسع عشرة صورة تظهرها عارية بشكل كلي أو جزئي، جاء قرار المحكمة في 9 جوان 1998 ليضع على عاتق متعهد الإيواء التزاما ببذل العناية والجهد اللازمين لمراقبة احترام المواقع الإلكترونية المأوية لحقوق الآخرين وللآداب العامة، ويرتب مسؤوليته في حال إخلاله بهذا الالتزام استنادا إلى المادة 1383 من القانون المدني الفرنسي، وقد ورد في حيثيات قرار المحكمة شروط إعفاء متعهد الإيواء من المسؤولية والتي تمثلت بوجوب إثبات قيامه بإعلام أصحاب المواقع الإلكترونية المأوية بضرورة مراعاة القوانين والأنظمة السارية، وبعدم الاعتداء على حقوق الآخرين وحقوق الملكية الفكرية على الإنترنت، كما يجب عليه أن يثبت، أيضا، أنه قام بالإجراءات اللازمة من أجل التقاط المواقع الإلكترونية المأوية التي تحتوي على مضمون معلوماتي غير مشروع، فعلى حد تعبير المحكمة من يأوي البيانات والمعلومات، ويقوم ببثها إلى الجمهور يتجاوز، حتما، دوره كناقل فني بسيط للمادة المعلوماتية، ويتوجب عليه بالتالي تحمل المسؤولية الناجمة عن ممارسة هذا النشاط في حال انتهاك حقوق الغير. وقد تم التأكيد على هذا القرار في مرحلة الاستئناف من قِبل محكمة استئناف باريس.

وأمام محكمة بداية (نانتير)، كان الدور هذه المرة لعارضة الأزياء الفرنسية Lynda Lacoste، والتي توجهت للمحكمة للمطالبة بإدانة أربعة متعهدي إيواء لإيوائهم المباشر والدائم لعدد من الصور التي تظهرها بشكل فاضح، وعرضها على شبكة الإنترنت دون الحصول على موافقتها، جاء قرار المحكمة في هذه القضية ليُحدد، بشكل واضح وصريح، نوعية الالتزامات الملقاة على عاتق متعهدي الإيواء وليطالبهم بوجوب إثبات تقيدهم بالالتزامات الواقعة على عاتقهم، خاصة تلك المتعلقة بإعلام أصحاب المواقع الإلكترونية المأوية بضرورة احترام حقوق الآخرين، وبذلهم العناية والجهد اللازمين للكشف عن أي مضمون معلوماتي غير مشروع، والتوقف عن بثه حال التقاطه، وبقرارها هذا، حددت المحكمة مضمون الالتزامات التي تقع

إن التزام متعهد الإيواء بالإعلام يفرض عليه أن يعلم أصحاب المواقع الإلكترونية المأوية بضرورة احترام القوانين والأنظمة، وعدم الاعتداء على حقوق الملكية الفكرية، ووجوب عدم إلحاق الضرر بالآخرين، بالمقابل فقد أكدت المحكمة عدم التزام متعهدي الإيواء بالكشف عن هوية أصحاب المواقع الإلكترونية، وذلك لعدم إمكانيتهم من التأكد من المعلومات التي يدلي بها الأشخاص عندما يطلبون إيواء مواقعهم، حيث يتم الإدلاء بهذه المعلومات إلكترونيا عن طريق تعبئة نموذج معروض على شبكة الإنترنت، وكذلك لصعوبة معرفة الرمز التعريفي IP (Internet Protocol) للكمبيوتر المستخدم في إنشاء الموقع الإلكتروني ذي المضمون غير المشروع.

إلا أن المحكمة نفسها عدلت عن موقفها هذا، وقضت عام 2000، بمناسبة دعوى رفعها الاتحاد العام للطلبة اليهود في فرنسا UEJF ضد متعهد الإيواء Multimania نتيجة لإيوائه موقعا إلكترونيا تضمن عرض وبيع أغراض ورموز نازية، بأنه يتوجب على متعهد الإيواء، وبالتعاون مع متعهد الوصول، الكشف عن هوية صاحب الموقع الإلكتروني ذي المضمون المعلوماتي غير المشروع أو الضار.[1]

أما فيما يتعلق بالالتزام باليقظة، فإن عدم إلزام متعهدي الإيواء بممارسة الرقابة الدقيقة والعميقة على مضمون المواقع الإلكترونية التي يأوونها، لم يعفهم من ضرورة اتخاذ الإجراءات اللازمة لالتقاط أي موقع إلكتروني يتضمن، وبشكل ظاهر، نشاطا غير مشروع، وذلك بقصد تصحيح وضعه أو قطع الخدمة عنه، ففي قضية "Estelle Hallyday" أشارت المحكمة إلى التزام متعهدي الإيواء بالبحث عن المواقع الإلكترونية المخالفة للقانون أو تلك التي تلحق ضررا بالآخرين، ومن أجل القيام بذلك باشر بعض متعهدي الإيواء بإعداد نظام بحث آلي قادر على التقاط المواقع الإلكترونية المتضمنة لكلمات أو لصور ذات علاقة بمواضيع الجنس، أو الجمال، أو الشهرة، أو الأنوثة، أو العنصرية، وعند التقاط مثل هذا المضمون يتوجب على متعهد الإيواء اتخاذ الإجراءات الضرورية التي تُمكنه من إرغام صاحب هذا الموقع على إزالة المخالفة، وعلى احترام القانون وعدم الإساءة للآخرين، وذلك قبل مباشرته بإغلاقه، ومن أجل التأكد من عدم إمكانية تكرار المخالفة، أرغمت المحكمة، في

على عاتق متعهدي الإيواء، وحصرتها بثلاثة: أولها الالتزام بالإعلام، وثانيها الالتزام باليقظة، وثالثها الالتزام بوقف بث المضمون المعلوماتي غير المشروع، أو على حد تعبير المحكمة، وجوب اتخاذ موقف إيجابي.أحمد فرح، المرجع السابق، ص333.

[1] أحمد فرح، المرجع السابق، ص334.

قرارها الصادر في قضية "Lynda Lacoste"، متعهدي الإيواء على البحث عن جميع الصور الفاضحة موضوع الدعوى وعلى إزالتها من على جميع صفحات الويب.

وقد وجدت المحكمة الابتدائية لمدينة (نانتير) في القواعد العامة في المسؤولية، وبخاصة نص المادتين: 1382 و1383 من القانون المدني الفرنسي، أساسا لمحمل قرارها هذا، وبالنسبة للمحكمة فإن تأسيسها على القواعد العامة يأتي كنتيجة طبيعية لغياب التنظيم القانوني الدولي للمسألة في ذلك الوقت، وأكدت محكمة بداية (نانتير) على موقفها السابق، من حيث نوعية الالتزامات التي ألقتها على عاتق متعهدي الإيواء وأساسها القانوني،[1] وفي قرار آخر أصدرته عام 2000 في الدعوى التي رفعها الاتحاد العام للطلبة اليهود في فرنسا ضد متعهد الإيواء وشددت في الوقت نفسه، على وجوب عدم إلزام متعهد الإيواء بممارسة الرقابة الدقيقة على مضمون المواقع الإلكترونية التي يأويها.[2]

إن تصدي القضاء لتحديد نطاق التزامات متعهدي الإيواء ومضمونه كان محلا للنقد من قبلهم، إلا إنه كان خطوة في الاتجاه الصحيح، ولأدل على ذلك من تبني المشرع الأوروبي، ومن بعده الفرنسي، للمبادئ التي استقر عليها القضاء في هذا المجال.

يبدو من الاتجاه العام لأحكام القضاء السابقة، أنها تميل إلى إلزام متعهدي الإيواء ببذل العناية اللازمة لمنع تداول المضمون أو المعلومات غير المشروعة، وذلك من خلال الجهود اليقظة التي تتناسب وإمكانياتهم، إلا أن مضمون هذه الجهود ومداها يبقى غامضا، فنص المادة 6-1/7 من القانون الفرنسي حول "الثقة في الاقتصاد الرقمي"[3] والذي جاء متفقا مع نص المادة 15-1 من التوجيه الأوروبي حول "التجارة الإلكترونية" يمنع فرض التزام عام على متعهد الإيواء "بمراقبة المعلومات التي يتولى نقلها أو تخزينها، أو البحث النشيط عن الوقائع والظروف التي تكشف عن الأنشطة غير المشروعة"، فبموجب هذا النص يجد متعهدو الإيواء أنفسهم أنهم يُعفون، على السواء، من ممارسة

[1] أحمد فرح، المرجع السابق، ص335.

[2] م عبد المهدي كاظم ناصر، المسؤولية المدنية لوسطاء الانترنت، مجلة القادسية للقانون والعلوم السياسية، العدد الثاني، المجلد الثاني، كانون الأول 2009، ص237.

[3] Les personnes mentionnées aux 1 et 2 ne sont pas soumises à une obligation générale de surveiller les informations qu'elles transmettent ou stockent, ni à une obligation générale de rechercher des faits ou des circonstances révélant des activités illicites.

الرقابة السابقة على المضمون المعلوماتي غير المشروع، ومن الصعوبات التقنية والاقتصادية التي تصاحب هذه الرقابة، والتي شكك البعض بفاعليتها.

غير أنه، وبحسب نص الفقرة الثانية من المادة 6-7/1[1] من القانون الفرنسي حول "الثقة في الاقتصاد الرقمي" والتي جاءت متفقة مع أحكام التوضيح رقم 47 من التوجيه الأوروبي حول "التجارة الإلكترونية"، فإن عدم فرض التزام عام على متعهد الإيواء بمراقبة المضمون المتداول عبر شبكة الإنترنت، لا يعفيه من الالتزام بممارسة هذه الرقابة في حالات خاصة، بمعنى أنه لا يعفيه من القيام "بنشاط رقابي موجه ومؤقت بناء على طلب السلطة القضائية"، وقد أثار هذا الأمر حفيظة القائمين على هذه الخدمة، ووصل ببعضهم إلى حد القول بأن هذا الموقف يتسم بالتشدد في مواجهتهم، لا سيما وأن الفقرة الرابعة من نص المادة 6-7/1، من القانون نفسه، تزيد من شدة هذا الالتزام بوضعها على عاتقهم التزاما من نوع آخر يتمثل، من ناحية، في وجوب تأمين الوسائل التقنية اللازمة لمنع نشر مضمون معلوماتي غير مشروع وتداوله عبر شبكة الإنترنت، ومن ناحية أخرى في ضرورة إعداد وسيلة اتصال مفتوحة من شأنها أن تربطهم مباشرة بمستخدمي الإنترنت، وتُمكنهم، في الوقت نفسه، من تبليغ السلطات العامة في الدولة عن أي مضمون إلكتروني مخالف للقانون.[2]

واتخاذ مثل هذا الموقف من قِبل المشرع الفرنسي لم يأتِ إلا تطبيقا لمبدأ أرسته المادة 15-2 من التوجيه الأوروبي حول "التجارة الإلكترونية"، والذي بدوره لم يغفل التزام متعهد الإيواء بممارسة الرقابة اللاحقة على المضمون المعلوماتي غير المشروع، فسمح للدول الأعضاء بأن تفرض على متعهد الإيواء

---

[1] Le précédent alinéa est sans préjudice de toute activité de surveillance ciblée et temporaire demandée par l'autorité judiciaire.
Compte tenu de l'intérêt général attaché à la répression de l'apologie des crimes contre l'humanité, de l'incitation à la haine raciale ainsi que de la pornographie enfantine, de l'incitation à la violence, notamment l'incitation aux violences faites aux femmes, ainsi que des atteintes à la dignité humaine, les personnes mentionnées ci-dessus doivent concourir à la lutte contre la diffusion des infractions visées aux cinquième et huitième alinéas de l'article 24 de la loi du 29 juillet 1881 sur la liberté de la presse et aux articles 227-23 et 227-24 du code pénal.
A ce titre, elles doivent mettre en place un dispositif facilement accessible et visible permettant à toute personne de porter à leur connaissance ce type de données. Elles ont également l'obligation, d'une part, d'informer promptement les autorités publiques compétentes de toutes activités illicites mentionnées à l'alinéa précédent qui leur seraient signalées et qu'exerceraient les destinataires de leurs services, et, d'autre part, de rendre publics les moyens qu'elles consacrent à la lutte contre ces activités illicites.
Compte tenu de l'intérêt général attaché à la répression des activités illégales de jeux d'argent, les personnes mentionnées aux 1 et 2 mettent en place, dans des conditions fixées par décret, un dispositif facilement accessible et visible permettant de signaler à leurs abonnés les services de communication au public en ligne tenus pour répréhensibles par les autorités publiques compétentes en la matière. Elles informent également leurs abonnés des risques encourus par eux du fait d'actes de jeux réalisés en violation de la loi.

[2] أحمد فرح، المرجع السابق، ص337.

التزاما بإعلام السلطات العامة في الدولة، وذلك بصورة عاجلة، عن أية نشاطات أو معلومات غير مشروعة، كما طالبهم بالكشف عن البيانات والمعلومات التي تسمح بتحديد شخصية صاحب المضمون، وتطبيقاً لذلك جاءت المادة 6-2 من القانون الفرنسي حول "الثقة في الاقتصاد الرقمي" لتُؤكد على التزام متعهد الإيواء بطلب البيانات والمعلومات الخاصة بعملائه، والاحتفاظ بها من أجل اطلاع السلطة القضائية عليها عند الطلب، وهذا الالتزام هو التزام تبادلي، بمعنى أن صاحب المضمون يلتزم من جهته بتزويد متعهد الإيواء بالبيانات والمعلومات المطلوبة، والتي تسمح بتحديد هويته، وبالمقابل على متعهد الإيواء، وفقا لنص المادة 6-1/3 و2 من القانون الفرنسي الاحتفاظ بها سرية وعدم إساءة استخدامها وعدم الكشف عنها إلا للضرورة، وقد أعطت الفقرة الخامسة من نص المادة 6-2، من القانون نفسه، بمجلس الدولة تبني نظام قانوني غايته تحديد البيانات والمعلومات الواجب على متعهد الإيواء حفظها وتحديد مدة هذا الحفظ وطريقته، وفي انتظار اتخاذ المجلس لهذه الخطوة، ومن أجل سد الفراغ القانوني الحاصل في هذا المجال، لم يكن أمام المحاكم الفرنسية وأمام القائمين على هذه الخدمة من سبيل سوى اللجوء إلى القواعد العامة في قانون الإجراءات المدنية، فاستناداً لنص المادتين: 809 و872 من قانون أصول المحاكمات المدنية الفرنسي الجديد لرئيس محكمة البداية، بصفته قاضي الأمور المستعجلة اتخاذ الإجراءات الملائمة لحفظ أدلة الإثبات. [1]

فعلا صدر المرسوم 2011-219 في 2011/02/25 المتعلق بحفظ ونقل المعطيات، المتعلقة بالتعرف على كل شخص أسهم في وضع محتوى على الخط،[2] أجبر متعهدي الإيواء ومزودي الخدمة على حفظ، ولمدة سنة، مجموعة من المعطيات الشخصية المتعلقة بالعميل، حتى تتمكن السلطات المختصة من معرفة كل مستخدم للانترنت ينشر معلومات غير مشروعة على الويب، مزودو الخدمة يقومون بالحفظ بالنسبة لكل استعمال للانترنت بالنسبة لعملائهم، ومتعهدو الإيواء بالنسبة لكل عملية إنشاء محتوى.[3]

إن مورد المعلومات هو صاحب السلطة الحقيقية في مراقبة المادة المعلوماتية التي تُبث عبر الإنترنت؛ لأنه هو من يقوم بجمعها أو تأليفها، وبالتالي يقع على عاتقه توريد مادة معلوماتية مشروعة وحقيقية. وعليه، يتعين على مورد المعلومات، الحريص على أداء دوره في إدارة شبكة الإنترنت

[1] أحمد فرح، المرجع السابق، ص338.

[2] Décret 2011-219 du 25/02/2011 relatif à la conservation et à la communication des données permettant d'identifier toute personne ayant contribuer à la création d'un contenu mis en ligne.

[3] Romain V. Gola, op cit, p486.

بمسؤولية وشفافية، إبلاغ السلطات المختصة في الدولة عن أي نشاط معلوماتي غير مشروع، كما يتوجب عليه الكشف عن هوية جميع القائمين على المضمون المعلوماتي المورد عبر الإنترنت، وهو ما يدخل تحت باب التزامه بممارسة عمله بشفافية، وكذلك يتوجب على مورد المعلومات السماح للجمهور بممارسة حق الرد.[1]

لكونه ناشرا للمعلومات على الموقع الإلكتروني، وبالتالي صاحب القدرة الفعلية في السيطرة عليها والتحكم في نشرها، يتحمّل مورد المعلومات المسؤولية بالدرجة الأولى عن مضمون الرسائل والمعلومات والصور التي يبثها، فهو ملتزم مثل مورد المضمون المعلوماتي التقليدي بمراقبة المضمون المعلوماتي الذي يصل إليه، وسلطة المراقبة هذه تتفق مع طبيعة عمله كناشر إلكتروني للمادة المعلوماتية، وبالنظر إلى طبيعة عمله، فإنه ملزم بإخطار السلطات المختصة في الدولة عن أي نشاط إلكتروني غير مشروع، وذلك من خلال مدير النشر المسؤول، فيجب عليه تعيين شخص طبيعي مدير للنشر، فضلا عن ذلك وتطبيقا لمبدأ الشفافية، يتوجب على مورد المعلومات اطلاع مستخدمي الإنترنت ومتعهدي الوصول والإيواء على البيانات والمعلومات التي تُعرف به وبالنشاط الإلكتروني الذي يديره. ومن عناصر التعريف التي يلتزم مورد المعلومات تقديمها:

- إذا كان مورد المعلومات شخصا طبيعيا، يجب عليه التعريف باسمه، وكنيته، وعنوانه، أما إذا كان شخصا معنويا فيلتزم بالتعريف باسم الشخص المعنوي، وطبيعة نشاطه، ومركز إدارته الرئيسي.
- على مورد المعلومات أيضا، تعيين مدير للنشر، وعند الضرورة رئيسا للتحرير، وعليه كذلك، طبقا لنص المادة 6-1/3 من القانون الفرنسي حول "الثقة في الاقتصاد الرقمي"، الكشف عن اسم متعهد الإيواء ولقبه، أو عنوانه ومركز إدارته الرئيس.

إن هذه العناصر يجب أن تكون ظاهرة للعيان ومنشورة على الصفحة الرئيسة للموقع الإلكتروني، أو على الأقل من الممكن الوصول إليها، من خلال الضغط على أيقونة أو إشارة، أو علاقة معينة أعدت خصيصا لهذا الغرض، كذلك يتوجب على مورد المعلومات تأمين الوسائل التقنية اللازمة للتعريف بصاحب المضمون غير المشروع، ومن المؤكد أن ذلك لا يُثير لمورد المعلومات أية إشكاليات نظرا لوجود رمز تعريفي (IP) واسم موقع إلكتروني لكل حاسب آلي مرتبط بشبكة

[1] محمد حسين منصور، المرجع السابق، ص179.

الإنترنت، والتعامل مع هذه البيانات والمعلومات، بحسب نص الفقرة الثانية من المادة 6-2/3 من القانون الفرنسي حول "الثقة في الاقتصاد الرقمي"، لا بد أن يتم بسرية بالغة، ويجب عدم الكشف عن هذه المعلومات إلا للضرورة.[1]

إن تقيد مورد المعلومات بجميع التزاماته السابقة، من رقابة على المضمون المعلوماتي، وتعيين مدير للنشر، والكشف عن جميع عناصر التعريف المطلوبة منه، يجعل من الشفافية طابعا لعمله، الأمر الذي يصعب معه ملاحقته أو إدانته، على أن هذا لا يعني إعفاءه، بأي حال من الأحوال، من إتاحة حق الرد لأي مستخدم إنترنت يثبت بطريقة أو بأخرى أن المادة المعلوماتية المنشورة على الشبكة تُشكل مساسا بحقوقه.

وفقا للقانون الفرنسي حول "الثقة في الاقتصاد الرقمي، يتمتع كل شخص طبيعي أو معنوي بحق الرد على أية مادة معلوماتية منشورة على شبكة الإنترنت، تمس بشرفه، أو بسمعته، أو تنتهك حقوقه، ويجب عليه أن يقدم هذا الرد إلى مدير النشر المسؤول خلال مدة أقصاها ثلاثة شهور تبدأ من تاريخ وقف بث المضمون غير المشروع على شبكة الإنترنت، وليس من تاريخ بدء البث، كذلك يقع على عاتق مورد المعلومات التزام عام بتأمين الوسائل التقنية والمعلوماتية اللازمة لتمكين الشخص المضرور من ممارسة هذا الحق، وبالتالي من نشر رده مباشرة على شبكة الإنترنت،كما يجب عليه، وتحت طائلة المسؤولية، تمكين الشخص المضرور من المطالبة بتصحيح أو حتى بشطب المادة المعلوماتية غير المشروعة من على صفحات الويب.[2]

غير أنه ليس من العدل إلقاء كامل المسؤولية على مورد المادة المعلوماتية غير المشروعة وحده، فهناك أكثر من شخص يتدخل في العملية، ومن الممكن بالتالي قيام مسؤوليتهم في حال ثبوت خرقهم لأي من الالتزامات الملقاة على عاتقهم، ومن هؤلاء الأشخاص الذين يقدمون الخدمة الفنية.

[1] عبد المهدي كاظم ناصر، المرجع السابق، ص241.

[2] أحمد فرح، المرجع السابق، ص 344.

ثانيا: التزامات مقدمي الخدمة الفنية.

مقدمو الخدمة الفنية هم أشخاص طبيعيون، أو معنويون يقومون بدور فني بحت لربط شبكات الاتصال من ناحية، ولتوصيل الجمهور إلى شبكة الإنترنت من ناحية أخرى، ويتم ذلك بموجب عقدين مختلفين: الأول، يتمثل في عقد نقل المعلومات، ويتولى الناقل بمقتضاه عملية الربط الفني بين شبكات الاتصال، في حين يهدف الثاني، من خلال متعهد الوصول، إلى تأمين توصيل العميل إلى الموقع الإلكتروني المنشود.

إن عملية نقل المعلومات عبر الإنترنت تقتضي، ربط حاسبات مستخدمي الشبكة بالمواقع الإلكترونية، وذلك من خلال الربط المادي لشبكات الاتصال عن بعد، ويلتزم ناقل المعلومات، بموجب عقد النقل الذي يربطه بعملائه، بتقديم الوسائل التقنية والفنية اللازمة لعملية النقل المادي للمضمون المعلوماتي. ودوره ينحصر في النقل المادي للمعلومات بين الوحدات المختلفة، ولا يُفترض به مراقبة المعلومات التي تمر عبر شبكته، ولا يكون بالتالي مسؤولا عن عدم مشروعية المادة المعلوماتية المتداولة، وأكثر من ذلك، إن ناقل المعلومات مطالب بالحفاظ على سرية المعلومات التي تمر من خلال شبكته، ومطالب، أيضا، بالحياد التام تجاه المضمون المعلوماتي المنقول.[1]

ولكن، هل يبقى الحال كذلك فيما لو علم ناقل المعلومات بعدم مشروعية الرسائل والمعلومات المقدمة؟ إن علم الناقل بأوجه عدم المشروعية للمضمون المعلوماتي وبالرغم من ذلك نقله له عبر شبكته، يُشكل إخلالا بالتزامه بضمان احترام نصوص النظام العام، وبواجب الحرص على عدم المساس بحقوق الآخرين.

ويثور التساؤل هنا حول مدى شرعية النسخ المؤقت للمضمون المعلوماتي المنقول والذي يقوم به ناقل المعلومات كجزء من عمله، وكخطوة تمهيدية وضرورية لنقل الرسائل والمعلومات عبر شبكة الإنترنت، وفقا لنص المواد 1-3/1 و 2-2/1 من القانون الفرنسي الصادر في الفاتح أوت 2006، و5-1/أ وتوضيحها رقم 33 من التوجيه الأوروبي الصادر بتاريخ 22 مايو 2001 والمتعلقين بحق المؤلف والحقوق المجاورة له في مجال المعلوماتية، إن عملية النسخ المؤقت لا تُشكل انتهاكا لحق المؤلف والحقوق المجاورة له، بشرط انحصار العملية في نطاق وحدود وضرورة إيصال المعلومات كما هي

[1] بيومي حجازي، المرجع السابق، ص151.

دون إجراء أي تعديل أو تحديث عليها من قِبل ناقل المعلومات؛ أي دون التأثير على حق مؤلف المضمون، خاصة إذا ما التزم الناقل بسحب النسخة التي تم تخزينها بشكل مؤقت، وبمنع الوصول إليها في حال أن علم بصدور قرار قضائي أو إداري يقضي بعدم مشروعية المضمون المخزن. وما يُمكن ملاحظته، بهذا الصدد، أن آلية عمل ناقل المعلومات قريبة جدا من آلية عمل والتزامات متعهد الوصول والتزاماته.[1]

نظرا لارتباطه الدائم بشبكة الإنترنت ولطبيعة الخدمة التي يقدمها، يُعد متعهد الوصول واحدا من أهم مقدمي الخدمات في العالم الافتراضي، فنشاطه الرئيس يتمحور في تزويد مشتركيه بالوسائل الفنية اللازمة لربطهم بشبكة الإنترنت، ولإبحارهم فيها بحرية ولوصولهم إلى المواقع الإلكترونية التي يريدون الإطلاع على مضمونها، ويُفترض في متعهد الوصول المسؤول احترام التزاماته الجوهرية، الإعلامية منها والتقنية.

وفقا لأحكام القانون والقضاء، يتوجب على متعهدي الوصول ممارسة عملهم بكل شفافية ووضوح، وبما يتلاءم مع مقتضيات حسن النية، ومن أجل تحقيق ذلك، ألزمت هذه الأحكام متعهدي الوصول بلعب دور إعلامي إيجابي في إدارة شبكة الإنترنت، وأقامت مسؤوليتهم على عدم أدائه، وعليه فقد أصبح لزاما على متعهدي الوصول، من ناحية، إعلام مستخدمي الشبكة بالبيانات والمعلومات الخاصة بهم وبالمشتركين معهم، ومن ناحية أخرى، توعية المشتركين بمخاطر الإبحار عبر الإنترنت، وإعلامهم بوجوب احترام القوانين والأنظمة السارية، وبعدم الاعتداء على حقوق الغير أثناء هذا الإبحار.[2]

وفيما يخص التزام متعهدي الوصول بالإعلام، أو الكشف عن البيانات والمعلومات الخاصة بهم وبالمشتركين معهم، فمن المعلوم أن القواعد العامة في التعاقد تُوجب تحديد هوية المتعاقدين، ولم يخرج عقد تقديم خدمات الدخول عن هذه القاعدة، إلا أن عملية إبرام هذا النوع من العقود وطرق تنفيذه عادة ما تتم عن طريق الإنترنت، الأمر الذي ينتج عنه بعض الصعوبات في تحديد هوية أطرافه، لذا، يتوجب على متعهد الوصول، الذي يعرض خدماته على المستهلكين أو المهنيين، احترام

[1] أحمد فرح، المرجع السابق، ص346.

[2] بيومي حجازي، المرجع السابق، ص138.

القواعد العامة في حماية المستهلك وقواعد القانون التجاري التي تفرض على كل شخص، يتخذ من تقديم خدمات الإنترنت مهنة له التعريف بنفسه لجمهور المتعاملين، فوفقا لنص المادتين: 5 من التوجيه الأُوروبي حول "التجارة الإلكترونية"، و6-1/3 من القانون الفرنسي حول "الثقة في الاقتصاد الرقمي: " على متعهد الوصول الكشف لعملائه، على الأقل، عن اسمه وعنوانه البريدي والإلكتروني، ومكان ورقم قيده التجاري"، فالإطلاع على هذه المعلومات يضفي حماية فعالة على جمهور المتعاملين عند إخلال متعهد الوصول بأي من التزاماته.[1]

وفي المقابل، يقع على عاتق متعهد الوصول، الطلب من عملائه، وذلك في المرحلة ما قبل التعاقدية، تقديم جميع البيانات والمعلومات الشخصية التي تُمكنه من تحديد هوية العميل، وأهليته، وعنوان بريده الالكتروني، كما يتوجب عليه، تحديد آلية جمع هذه المعلومات، أي الوسيلة التي يمكن للعميل من خلالها تزويد متعهد الوصول بالبيانات والمعلومات المطلوبة. ويثور السؤال هنا حول كيفية تأكد متعهد الوصول من صدق البيانات والمعلومات المقدمة من قِبل العميل، في حال إخلال هذا الأخير بالتزامه بعدم خرق القوانين والأنظمة السارية، وباحترام حقوق الآخرين على شبكة الإنترنت، خاصة أن تقديمها يتم عن طريق الإنترنت.

إن النصوص القانونية الحالية على الصعيدين الأُوروبي والفرنسي لا تُلزم متعهدي الوصول بضرورة التأكد من صدق البيانات والمعلومات المقدمة من قِبل العميل عبر الإنترنت، إلا إن الواقع يُثبت اتباع متعهدي الوصول لآلية تسجيل دقيقة للعملاء على مواقعهم الإلكترونية، ليس هذا فحسب فهم يقومون أيضا بعملية حجب آلي لمفتاح الدخول لشبكة الإنترنت، وذلك بغية إرساله له على عنوانه الإلكتروني المعلن، ولا يتم حصول العميل على هذا المفتاح إلا بعد دخوله إلى بريده الإلكتروني وقراءة الرسالة الموجهة إليه من متعهد الوصول الذي تعاقد معه، غير أن العميل سيء النية بإمكانه التغلب على هذه الآلية، وذلك عن طريق إجراء عملية تسجيل بريد إلكتروني وهمي من خلال تقديم بيانات ومعلومات غير صحيحة.

ومن ناحية أخرى، يوجب القضاء الفرنسي على متعهدي الوصول، وذلك تنفيذا لعقد تقديم خدمات الدخول، تبصرة العملاء بالمخاطر التي من الممكن أن يتعرضوا لها خلال عملية

[1] محمد حسين منصور، المرجع السابق، ص179.

إبحارهم في عالم الإنترنت ودخولهم إلى مواقع إلكترونية معينة أو التعامل معها، كما يضع على عاتقهم الالتزام بإعلام عملائهم بضرورة احترام القوانين والأنظمة السارية، ووجوب عدم استخدام شبكة الإنترنت كوسيلة للاعتداء على حقوق الغير، كذلك يتوجب على متعهدي الوصول، وفقا لنص المادة 3/14 من التوجيه الأوروبي حول "التجارة الإلكترونية"، وانطلاقا من مبدأ حسن النية في إدارة شبكة الإنترنت، التعاون مع جميع المعنيين بالخدمات المقدمة على الشبكة من جهات إدارية وقضائية، ومن جمهور المستخدِمين، ومن العاملين في قطاع خدمات الإنترنت. ويأتي هذا الالتزام مكملا لالتزاماته الأخرى ذات الطبيعة التقنية.

جاءت أحكام القضاء الفرنسي في هذا المجال لتؤكد هذا الدور ولتُقرر انحصار دور متعهد الوصول في تأمين نقل البيانات والمعلومات بطريقة فورية، وبالتالي لا يقع على عاتقه التزام عام بمراقبة مضمون المادة المعلوماتية التي تمر من خلاله.

المشرع الأوروبي بدوره أعلن في المادة 15-1 من التوجيه الأوروبي حول "التجارة الإلكترونية" أنه يحظر على الدول الأعضاء فرض التزام عام على مقدمي خدمات الإنترنت برقابة المعلومات التي يتولون نقلها أو تخزينها، أو التزام بالبحث النشيط عن الوقائع والظروف التي تكشف عن الأنشطة غير المشروعة، وباعتبار فرنسا إحدى الدول الأعضاء في الاتحاد الأُوروبي كان لزاما على المشرع الفرنسي تبني موقف مطابق لموقف المشرِع الأوروبي، وتم ذلك بالفعل، فجاء نص المادة 6-7/1 من القانون الفرنسي حول "الثقة في الاقتصاد الرقمي" ليضع على عاتق متعهدي الوصول التزاما بالحياد التام فقط، وبالتالي عدم التدخل في مضمون المادة المعلوماتية المنقولة، مع ما يتطلبه ذلك، بحسب نص المادة 6-2/3 من نفس القانون، من وجوب المحافظة على سرِية الاتصالات، وعدم الكشف عن مضمونها إلا للسلطة القضائية المختصة عند الضرورة.[1]

غير أن التزام متعهدي الوصول بالحياد التام لا يُعفيهم، من الالتزام بممارسة الرقابة الموجهة والمؤقتة للمعلومات التي تمر من خلالهم، بناء على أمر صادر من السلطة القضائية المختصة، ومن واجب تبليغ السلطات العامة في الدولة عن أي مضمون إلكتروني غير مشروع.

[1] أحمد فرح، المرجع السابق، ص 346.

نوع آخر من الالتزامات يقع على عاتق متعهدي الوصول، يتمثل في وجوب اقتراحهم على عملائهم الوسائل الفنية اللازمة لمنع الوصول إلى بعض المواقع الإلكترونية المشبوهة.

الفرع الثالث: مسؤولية مقدمي خدمات الإنترنت عما يحدث من مخالفات عبر الشبكة.

إن تحديد مسؤولية مقدمي خدمات الإنترنت يعد من أصعب المواضيع الممكن مواجهتها، ومرد ذلك لعدة أسباب: منها الطابع الفني المعقد للشبكة، وعالمية النشاط الإلكتروني غير الخاضع لسيطرة دولة معينة أو لإدارة مركزية، وتعدد الهيئات التي تعرض خدماتها في هذا المجال، ووجود كم كبير من المتدخلين في تسيير هذه الشبكة...

إزاء هذه المخالفات المتعددة يثور السؤال حول الطريقة الأنسب لمعالجتها، فهل من الأمثل الأخذ بعين الاعتبار خصوصية بعض المخالفات، كتلك المتعلقة بحقوق الملكية الفكرية مثلا، وبالتالي تخصيص النصوص القانونية لمعالجة كل مخالفة وحدها؟ أم من الأفضل وضع قواعد عامة للمسؤولية عن المخالفات المرتكبة على الإنترنت بصرف النظر عن مضمونها؟

كان لتناول الصحافة المتكرر لمسألة انتهاك حرمة الحياة الخاصة، وقداسة الأديان على شبكة الإنترنت الأثر الأكبر في انتشار الحديث عن المسؤولية الجزائية لمقدمي خدمات الإنترنت.[1]

وقد اختلف مسلك التشريعات فيما يتعلق بمسؤولية الوسطاء في الانترنت، فوفقا للقانون الأمريكي وما استقر عليه القضاء تقوم مسؤولية الموزع على أساس القواعد العامة، أو على أساس عدم قيامه بواجب الرقابة، حسب الحالة، وقد خلت القوانين العربية تقريبا من نصوص تنظم مسؤولية هؤلاء الوسطاء.[2]

أولا: المسؤولية الجزائية لمتعهد الوصول

تعددت الآراء الفقهية حول مسؤولية متعهد الوصول الجزائية، سواء باعتباره فاعلا في الجريمة أو شريكا، وانقسم الفقه بشأن هذه المسألة إلى ثلاثة اتجاهات، بحيث يرى الاتجاه الأول عدم مساءلة متعهد الوصول حتى ولو قام بدور متعهد الإيواء، لأنه يقوم بعمل فني صرف، كما أنه ليس

[1] بيومي حجازي، المرجع السابق، ص132.

[2] المرجع نفسه، ص135

قاضيا ليقرر ما إذا كان المحتوى مشروعا أم لا، مما يفرض عليه عدم مراقبة المحتوى أو محوه، ولكن وجهت انتقادات لهذا الرأي،[1] لذا يرى أصحاب الاتجاه الثاني مساءلة متعهد الوصولFAI ، على أساس المسؤولية التوجيهية، باعتباره أحد الأشخاص ضمن سلسلة وضعها المشرع، مما يوجب عليه منع أو محو المحتوى غير المشروع، ولا يجوز له التذرع بجهله أو عدم معرفته لهذا المحتوى غير المشروع،[2] لذلك يرى أصحاب الاتجاه الثالث أن مساءلة FAI من عدمها يتوقف على طبيعة الدور الذي يقوم به هذا المتعهد.

أما بالنسبة لمساءلة FAI كشريك في الجريمة، فإن أفعال الاشتراك لا تتوافر في حقه، فهو لا يقوم بتوصيل الجاني بالموقع حيث يوجد المحتوى غير المشروع، إنما يقوم بتوصيل المشترك إلى الموقع الذي يريده، كذلك فإن وضع المحتوى غير المشروع على الشبكة يمكن تحققه قبل ربط المشترك بالموقع عن طريق FAI بل قد يكون موجودا قبلFAI نفسه. كما أن القصد الجنائي غير متوفر أيضا.[3]

عرضت أمام القضاء بعض القضايا التي استلهم منها المشرع الفرنسي فيما بعد المبادئ التي جاء بها قانون LCEN. [4]

---

[1] أ. د. جميل عبد الباقي الصغير، الانترنت والقانون الجنائي، دار النهضة العربية، القاهرة، مصر 2012، ص135.

من الانتقادات التي وجهت لهذا الاتجاه أنه غير صحيح وبه مغالطات، فمتعهد الوصول قد يلعب دورا إيجابيا من الطبيعة ذاتها التي يقدمها مقدم المعلومات أو المنتج، بحيث أن دوره لا يقتصر على إرسال المعلومات، ولكنه يقترح المحتوى أيضا، والموقف هنا مشابه لما يحدث في الصحافة المكتوبة، حيث يمكن للشخص الواحد القيام بوظائف عديدة، وفي هذه الحالة يسأل متعهد الوصول عن المعلومات غير المشروعة إذا قام بوضعها على الانترنت. المرجع نفسه، ص136.

[2] انتقد هذا الرأي أيضا، فمساءلة متعهد الوصول على أساس المسؤولية بالتعاقب يؤدي حتما إلى مساءلة مدير مكتب البريد أو الهاتف عن المراسلات غير المشروعة التي توجد بالبريد أو المحادثات السيئة التي تحدث أثناء الاتصالات الهاتفية وهو ما لم يقل به أحد، كما أن متعهد الوصول باعتباره"رابطا فنيا" لا يمكنه مباشرة رقابة توجيهية على رسائل مشتركيه. المرجع نفسه، ص137.

[3] جميل عبد الباقي الصغير، المرجع السابق، ص154.

[4] رفعت دعاوى قضائية عديدة- في فرنسا وغيرها- ضد متعهد الوصول، سواء بسبب دوره كمرحل فني، أو بسبب الرسائل التي يبثها مشتركوه. فللمساهمة في المجموعات الإخبارية أو مؤتمرات المناقشة العامة يقوم مستخدمو الانترنت ببث رسائلهم على الحاسب الخادم الخاص بمتعهد الوصول، والذي يقوم بربطهم بعد ذلك بالحاسبات الخادمة الأخرى من النوع نفسه، فنقطة الانطلاق بالنسبة للنشر العلني للرسالة تبدأ إذن من الحاسب الخادم الخاص بمتعهد الوصول.

وهذه الحالة كانت محلا لثلاثة أحكام صدرت من القضاء الأمريكي في مجال القذف والاعتداء على حق المؤلف، آخر صدر عن المحاكم الهولندية، ويستخلص من هذه الأحكام عدة مبادئ هامة فيما يتعلق بمسئولية متعهدي الوصول. وسأذكر حكمين:

الحكم الأول صدر في قضية "CUBBY" ضد شركة "COMPUSERVE": من بين الخدمات التي تقدمها شركة " COMPUSERVE" لمشتركيها خدمة التوصيل لمؤتمرات عامة مختلفة. وأحد هذه المؤتمرات قد خصص لطباعة الصحف. وأحد المنشورات الجاهزة

خلاصة هذه الأحكام أنه لا يمكن إعمال قواعد المسئولية الجنائية المفترضة في حق موزع خدمة الانترنت لأن دوره فني بحت ينحصر في توصيل المشترك أو العميل بالمواقع التي يرغبها على شبكة الانترنت، وبالتالي فلا يحق له رقابة مشروعية المادة المعلوماتية التي يقوم بنقلها، فدوره يطابق تماما دور موزع البريد أو موظف التليفون الذي يقوم بتوصيل المشترك برقم معين يطلبه، وعليه يتوجب الرجوع للقواعد العامة للمسئولية الجزائية لإعمال مسؤولية موزع خدمة الانترنت بأن يثبت أن له دور إيجابي في بث مادة معلوماتية غير مشروعة وأن يتوافر لديه القصد الجنائي العام بعنصرية العلم والإدارة، فضلا عن ضرورة قدرته الفنية على رقابة المادة المعلوماتية التي تنقل عن طريقه.

كما يجب أن تقتصر هذه المسؤولية على الحالات التي يكون فيها الطابع غير المشروع واضحا مثل النسخ الكامل لأعمال فنان مشهور أو صور فاضحة.

عن هذا المؤتمر "RUMOVILLE USA" كانت تتضمن عبارات قذف في حق "CUBBY". وبالتالي ثار البحث في مسؤولية"COMPUSERVE"عن هذه العبارات التي تتضمن قذفا.

وشركة "COMPUSERVE" وإن كانت لم تذكر طابع القذف الذي تضمنته العبارات إلا أنه دفعت بعدم مسئوليتها لأنها لم تكن تعلم بعبارات القذف. وانتهت المحكمة إلى أنه لا يمكن أن يطلب من هذه الشركة أن تقوم بفحص كل منشور تقوم بنقله للكشف عن أي رسائل قد تتضمن قذفا.

والحكم الثاني صدر في قضية "STATTON OAKMONT" ضد شركة "PRODIGY": تتعلق هذه القضية بنشر رسالة تتضمن قذفا على أحد الندوات "FORUMS" الخاصة بشركة "PRODIGY". وهي متعهد خدمات مباشرة " FOURNISSEUR DE DERVICE EN LIGNE" مثل شركة "COMPUSERVE". وقد حكم في القضية بمسئولية شركة "PRODIGY" لأن القاضي الأمريكي قد أثبت أن هذه الشركة كانت تقدم نفسها للجمهور ولمشتركيها على أنها تمارس رقابة على محتوى الخدمات التي تقوم بتقديمها. بالإضافة إلى أن شركة "PRODIGY" كانت تمارس هذه الرقابة باستخدام برامج تنقيه"FILTRAGE" من نوعية خاصة وباتباع منهج معين يقوم به الأشخاص المكلفون بهذه الرقابة، وهذا يعني أن شركة "PRODIGY" كانت تمارس رقابة توجيهية على مؤتمرات المناقشة الخاصة بها، والذي كان من نتائجها قيام مسئوليتها عن عبارات القذف، وذلك على الرغم من أن الشركة "PRODIGY" قد تمسكت بأنه لا يمكنها أن تمارس رقابتها على 60000 رسالة يومية صادرة عن مشتركيها.

فالمحكمة اعتبرت أن هذه الشركة مثل الناشر في مجال الصحافة، وبالتالي فإنها تسأل دون حاجة إلى إقامة الدليل على أنها كانت تعلم بوجود المعلومات المجرمة على الشبكة. فالمسئولية هنا آلية تستنتج من وضعها كناشر.

ويفسر الخلاف بين الحكمين السابقين في أنه إذا التزم متعهد الوصول برقابة مشتركيه، فإن ذلك يؤدي إلى قيام مسئوليته. وبمناسبة قضية اتحاد الطلاب اليهود بباريس، فإن بعض متعهدي الوصول الفرنسيين قد تعهدوا بمراقبة مشتركيهم، وأن يبذلوا قصارى جهدهم لوقف الرسائل غير المشروعة أو فسخ عقد الخدمة الذي يربطهم بالمشترك، وأن يمنعوا بقدر المستطاع نشر المعلومات المجرمة التي تبث على صفحات الويب أو مؤتمرات المناقشة الخاصة بهم، والتي تقع بالمخالفة لقانون 29 يوليو 1881، وخاصة تلك المتعلقة بالعنصرية أو مقاومة السامية. ومع ذلك لم تطبق عليها المحكمة قواعد المسئولية التوجيهية. جميل عبد الباقي الصغير، المرجع السابق، ص139-141.

كما يجب على متعهد الوصول أن يقدم إلى سلطات التحقيق أية بيانات تتعلق بعملائه متى طلب منه ذلك، ولذلك يقوم متعهد الوصول بالحصول بيانات تحقيق الشخصية المتعلقة بأي مشترك قبل أن يسمح له بالاشتراك.

ويقع على عاتقه التزام بوقف بث المعلومات غير المشروعة متى كان لديه علم بطبيعتها الإجرامية وإلا قامت مسئولية الجنائية، ففي إحدى الوقائع، والتي حدثت في فرنسا، في غضون يناير 1996، تلقى قائد البحث بشرطة باريس بلاغا من قسم المعلومات الالكترونية بمعهد البحوث الجنائية بأن صورا خليعة تتعلق بالصغار تبث على الأراضي الفرنسية عبر شبكة الانترنت، وقد أشارت التحريات إلى اثنين من الموردين، وفتح محضر استدلالات، أعقبه قيام النيابة العامة بفتح تحقيق بتهمة إذاعة ونقل صور لقصر بعضهم أقل من خمسة عشر عاما ذات طابع خلاعي (م227-23 من قانون العقوبات الفرنسي)، ثم استمعت إلى أقوال مديري الموردين، وتم التحفظ على خمس أسطوانات تحمل ندوات مناقشة وختمت بالشمع الأحمر ضمن أحراز.[1]

ثانيا المسؤولية الجزائية لمتعهد الإيواء

في فرنسا يجوز مساءلة متعهد الإيواء على أساس القواعد العامة، كما يجوز مساءلته وفقا لقانون الصحافة والاتصال السمعي البصري؛ فحسب القواعد العامة يتعين التفرقة بين فرضين في مسؤولية متعهد الإيواء، الفرض الأول أن يكون متعهد الإيواء شريكا في جريمة بث الرسالة غير المشروعة، والفرض الثاني أن يسأل عن جريمة إخفاء أشياء مسروقة، ولكي يسأل متعهد الإيواء كشريك في جريمة بث المحتوى غير المشروع، لابد أن يثبت قيامه بفعل من أفعال الاشتراك وهي التحريض أو الاتفاق أو المساعدة، وصورة الاشتراك المتصورة هنا هي المساعدة، وذلك بأن يأتي أفعالا إيجابية تفيد مساهمته في السلوك الإجرامي للجريمة، وهذه ليست مفترضة، بل لا بد أن يقام عليها دليل مادي، يتمثل في علم متعهد الإيواء بالطابع غير المشروع للمحتوى، وذلك في وقت لاحق على اكتشاف هذه الرسالة غير المشروعة، ولذلك لا يسأل متعهد الإيواء متى ثبت عدم علمه بالمادة المعلوماتية غير المشروعة، لأن مجرد التعاقد مع مورد الرسالة أو المؤلف حتى ولو كانت غير مشروعة لا ينهض سببا لإدانته طالما أنه لم يعلم، فالجريمة عمدية، ولا تقوم مسؤولية متعهد الإيواء في الاشتراك

[1] بيومي حجازي، المرجع السابق، ص140.

استنادا للإهمال أو عدم الاحتراز، لأن صورة الركن المعنوي في هذه الجريمة، فقط هي العمد أي توافر القصد الجنائي دون الخطأ غير العمدي.

أما إذا كان متعهد الإيواء يعلم بالطابع غير المشروع للمادة المعلوماتية على الحاسب الخادم فإن مسؤوليته تتوقف على طبيعة الجريمة التي كانت هذه المعلومات موضوعا لها، هل هي جريمة وقتية أم جريمة مستمرة؟

إن بث رسالة إليكترونية غير مشروعة على قائمة المناقشة هي جريمة وقتية تتم في لحظة وجيزة، لذلك فعلم متعهد الإيواء بعدم مشروعية هذه المادة يجب أن يكون سابقا أو معاصرا للجريمة وليس لاحقا لها، وعلى العكس من ذلك لو كانت الجريمة مستمرة، فإن علم متعهد الإيواء بالمادة المعلوماتية غير المشروعة في أي وقت، تتحقق به صفة الاشتراك قبل متعهد الإيواء، كما في الجرائم التي ترتكب بواسطة الموقع (ويب)، ونفس الأمر ينطبق على الجرائم التي ترتكب على مواقع بروتوكول نقل الملفات عن بعد.[1]

في جريمة الإخفاء، لا بد أن تكون الأشياء التي تم إخفاؤها متحصلة من جريمة، ولذلك يفرق في هذه الجريمة بين حالتين، الأولى أن يقتصر دور متعهد الإيواء على مجرد وضع معلومات غير مشروعة على الذاكرة الحية للحاسب، فلا تقوم في حقه جريمة الإخفاء، لأن محكمة النقض في فرنسا كانت ترى أن المعلومات ليست كيانا ماديا يمكن حيازته وبالتالي لا يصلح أن يكون محلا للإخفاء، لكن إذا قام متعهد الإيواء بتسجيل المعلومات غير المشروعة على دعامة، ولتكن القرص الصلب للحاسب الخادم، ففي هذه الحالة يقوم في حقه جريمة الإخفاء.[2]

جاء القضاء الفرنسي ليقرر بأن مسؤولية مقدمي خدمات الإنترنت الجزائية يمكن أن تقوم على أساس التدخل في الجريمة أو الاشتراك فيها، ففي حكمها الصادر عام 1997، قالت محكمة باريس بأن مساهمة مقدم خدمات الإنترنت في بث مضمون معلوماتي غير مشروع، من الممكن أن يشكل تدخلا منه في ارتكاب الجريمة، الأمر الذي يستوجب معه إدانته إلى جانب الفاعل الأصلي

[1] بيومي حجازي، المرجع السابق، ص141.

[2] المرجع نفسه، ص143.

على هذا الفعل، وفي قرار لها صدر بتاريخ 28 مايو1998، أدانت محكمة صلح ميونخ الألمانية أحد مقدمي خدمات الإنترنت كشريك في جريمة نشر صور جنسية للأطفال على صفحات الويب.[1]

جاء المشرع الفرنسي متفقا بهذا الخصوص مع الاتجاه العام للتوجيه الأوروبي حول "التجارة الإلكترونية"، حيث نصت المادة 6-3/1 من القانون الفرنسي حول "الثقة في الاقتصاد الرقمي: "أن أفعال مقدمي خدمات الإنترنت الخاطئة لا يمكن أن تدخل في نطاق التجريم إلا إذا ثبت علمهم الفعلي بالمضمون الإلكتروني غير المشروع، وعلى الرغم من علمهم هذا لم يتخذوا الإجراءات اللازمة لشطبه، أو على الأقل لمنع وصول الجمهور إليه، وكذلك كانت لهم المكنة للقيام بذلك ولم يفعلوا.[2]

غير أنه وبالرجوع إلى نصوص قانون العقوبات الفرنسي، نجد بأنه لا يمكن أن يدان شخص بجريمة التدخل أو بالاشتراك الجرمي ما لم يثبت علمه بالأفعال المرتكبة، وتطبيقا لذلك، فإن القصد الجرمي لمقدمي خدمات الإنترنت ينتفي في حال ثبت عدم علمهم الفعلي بالمضمون الإلكتروني غير المشروع، أو إذا ما قاموا بمجرد علمهم بعدم مشروعية هذا المضمون، بشطبه، أو بمنع وصوله للجمهور إن كان بوسعهم ذلك.[3]

ولكي تنتفي مسؤولية مقدمي خدمات الإنترنت (متعهد الوصول ومتعهد الإيواء) الجزائية، بشكل كلي، وفي إطار مساعدتهم للسلطات العامة في الدولة في محاربة جرائم انتهاك حقوق الملكية الفكرية، وحرمة الحياة الخاصة وقداسة الأديان ... فإنهم مُطالبون، أيضا، وفقا لنص الفقرة الثالثة من المادة 6-7/2 من القانون الفرنسي حول "الثقة في الاقتصاد الرقمي"، والتي جاءت متفقة مع الاتجاه العام للمواد 13 و14 من التوجيه الأُوروبي حول "التجارة الإلكترونية"، ومع المادة 512/g/3 من القانون الأمريكي (DMCA)، والخاصة بالتعدي على حقوق الملكية الفكرية في نطاق الإنترنت، بأن يضعوا تحت تصرف عملائهم الوسائل اللازمة لتسهيل عملية التبليغ عن أي مخالفات قد تتم عبر الشبكة، وبعد تحقق مقدم الخدمات من صحة موضوع التبليغ ومن عدم مشروعية المضمون الإلكتروني عليه أن يُبادر فورا إلى إبلاغ السلطات العامة في الدولة عن هذه

[1] محمد حسين منصور، المرجع السابق، ص179.

[2] Pierre Sirinelli, la responsabilité des prestataires de l'internet, conférence de transaction électronique, p112.

[3] محمد حسين منصور، المرجع السابق، ص179.

الواقعة، وذلك من أجل استصدار أمر إداري أو قضائي بشطب هذا المضمون، أو منع وصوله لمستخدمي الشبكة.[1]

ويثور التساؤل حول وسيلة إثبات علم متعهد الإيواء بعدم مشروعية المضمون الإلكتروني الذي يأويه، لقد بين نص المادة السادسة المذكورة أعلاه بأن هذا العلم يثبت بمجرد أن يكشف له الشخص المتضرر طالب وقف البث عن هويته، ويحدد له المضمون المشتكى منه وأسباب عدم مشروعيته، ويُزوده بما يثبت قيامه بإرسال نسخة من طلب وقف المضمون غير المشروع إلى صاحبه أو مؤلفه، ولا بد أن يكون هذا التبليغ مُحدد التاريخ، لذا، فإنه يلزم لقيام مسؤولية متعهد الإيواء المرور بمرحلتين أساسيتين: بداية يجب إثبات علمه بعدم مشروعية المضمون الإلكتروني الذي يأويه، ويتم ذلك عادة من خلال الإخطار الذي يتم توجيهه إليه، ومن ثم إعطاؤه فرصة من أجل وقف البث، وفي حال عدم قيامه بذلك، فإنه يتحمل المسؤولية الناشئة عن خطئه الثابت.

ولكن كيف بالإمكان ضمان جدية التبليغ وبالتالي تجنب التبليغات التعسفية أو الكاذبة؟ أجابت عن هذا التساؤل المادة 6-4/1 من القانون الفرنسي حول "الثقة في الاقتصاد الرقمي"، والتي نصت على أن كل من بلغ مقدمي خدمات الإنترنت بوجود مضمون إلكتروني غير مشروع، من أجل شطبه أو منع الجمهور من الوصول إليه، مع علمه المسبق بعدم صحة تبليغه، يُعاقب بالسجن لمدة عام وبغرامة مقدارها خمس عشرة ألف يورو.

ثالثا: المسؤولية الجزائية للمنتج

يقصد به منتج الخدمة المعلوماتية في وسائل الاتصال السمعي البصري، وطبقا لأحكام القانون الفرنسي الصادر في 29 يوليو 1982 فإنه إذا ارتكبت جريمة من الجرائم المنصوص عليها في الفصل الرابع من القانون الصادر في 29 يوليو 1881 بواسطة وسيلة للاتصال السمعي البصري، فإن منتج الخدمة يجوز محاكمته كفاعل أصلي دون اشتراط أن تكون الرسالة غير المشروعة مسجلة بصفة مسبقة على توصيلها إلى الجمهور، وبناء عليه فإن رئيس الجمعية الذي بادر بإنشاء خدمة تليماتية (Télématique)، بهدف تبادل الآراء حول موضوعات محددة سلفا، يجوز أن يحاكم

[1] أحمد فرح، المرجع السابق، ص352.

بصفته منتجا لخدمة، دون أن يحق له أن يدفع بعدم إمكانية مباشرة الرقابة على محتوى الرسائل غير المشروع –وفقا لحكم محكمة النقض الفرنسية – في 1998/12/08.[1]

[1] Crim. 8 déc. 1998.

مشار إليه عند: جميل عبد الباقي، المرجع السابق، ص173.

وتتلخص وقائع هذه القضية في أن السيد "CR" مؤسس ورئيس جمعية اتحاد النهضة الفرنسية"CRF" بادر بفتح خدمة تليماتية " service télématique" أطلق عليها اسم "3615 Renouveau" من أجل السماح للتيارات الفكرية لليمين المسيحي بتبادل الآراء الدينية والسياسية. ومن أجل تحقيق هذا الهدف وبعد أن أعلن عن افتتاح هذه الخدمة للاتصال وقع السيد "CR" اتفاقية مع مركز خادم "Centre serveur" لوضع هذه الخدمة موضع التنفيذ، وذلك بوضع نظام يسمح بتوصيل الراغبين من خلال التليتل "Teletel" بالمؤتمر المعنى من أجل تسجيل آرائهم على الشاشة في وقت وجيز . ونظرا لأن محتوى الرسائل المجهولة، والتي نشرت في يومي22، 27 أبريل سنة 1994 على الموقع " 3615 Renouveau"على عنوان المؤتمر المعني كانت مرئية بالنسبة لمستخدمي المنيتل، فإن السيد "CR" قد قدم للمحاكمة على أساس المادتين 23، 1،3،6/24 من القانون الصادر في 29 يوليو سنة 1881 بصفته منتجا في مفهوم المادة 93-3 من قانون الاتصالات السمعية البصرية لسنة 1982، حيث ثبت أن بعض هذه الرسائل كانت تشكل تحريضا "Apologie" على الجرائم ضد الإنسانية، وعلى الاعتداء على الحق في الحياة وسلامة الجسم، وعلى التمييز العنصري.

ولما طرحت الواقعة على محكمة جنح استئناف "مون بيليه" قضت ببراءة المتهم "CR" ، وأسست حكمها على أن المنتج لا يسأل إلا إذا باشر رقابته أثناء عملية الإنتاج، وفي القضية الماثلة، فقد ثبت للمحكمة أن المتهم لم تكن له على الرسائل المسجلة على عنوان المؤتمر المعني أي سلطة رقابية، لا قبل ولا بعد توصيلها للجمهور، بحيث تسمح له بفحصها ومحو محتواها إذا كان غير مشروع. بمعنى أن المنتج لا يسأل بحسب المحكمة إلا إذا كان قادرا على مباشرة رقابته على الرسائل المنشورة، والمتهم"CR" لم تكن لديه هذه القدرة لا قبل ولا بعد توصيلها للجمهور.

إلا أن محكمة النقض الفرنسية قد نقضت في حكمها الصادر في 8 ديسمبر 1998 هذا الحكم، وقضت بأن المتهم "CR" يجب أن يحاكم بصفته منتجا، لأنه بادر بإنشاء خدمة للاتصال السمعي البصري من أجل تبادل الآراء حول موضوعات محددة سلفا، دون أن يكون له أن يدفع بأنه لم تكن لديه القدرة على مراقبة هذه الرسائل، وبحسب المحكمة، إذا ارتكبت إحدى الجرائم المنصوص عليها في القانون الصادر في 29 يوليو 1881 بواسطة الاتصال السمعي البصري (التليفيزيون)، فإن منتج الخدمة، يسأل في حالة عدم وجود مؤلف الرسالة غير المشروعة باعتباره فاعلا أصليا، حتى ولو لم تكن الرسالة مسجلة بصفة مسبقة على توصيلها للجمهور. فبحسب المحكمة يعتبر المتهم "CR" وقد بادر بإنشاء خدمة اتصال سمعي بصري من أجل تبادل الآراء حول موضوعات محددة سلفا، مسؤولا بصفته منتجا دون أن يكون له أن يدفع بأنه لم يباشر ثمة رقابة على الرسائل المجرمة. وبالتالي تكون محكمة النقض الفرنسية قد تبنت موقفا مختلفا جذريا عن موقف قضاء الموضوع (القضاء الابتدائي).

وبذلك تكون محكمة النقض قد أقرت بإمكانية تطبيق قانون 29 يوليو 1982، بشأن الاتصالات السمعية البصرية على شبكة الانترنت فالمتهم "CR" وقد بادر بافتتاح خدمة ووقع اتفاقية مع مركز خادم، فإنه يكون منتجا، وبهذه الصفة حوكم المتهم"CR" في مفهوم المادة 93-3-باعتباره فاعلا أصليا عن الجرائم المرتكبة، وإن كانت محكمة جنح استئناف قد برأته، لأنها لم تعتبر المتهم"CR" بمثابة منتج، حيث أنه لم تكن لديه القدرة على مباشرة أية رقابة أثناء عملية الإنتاج أما الدائرة الجنائية لمحكمة النقض في حكم8 ديسمبر 1998 فقد أكدت بأن المتهم "CR" وقد قام بخلق الخدمة المعينة، فإنه تكون له صفة المنتج. ولما كانت الفقرة الثانية من المادة 93-3 لا تتطلب لقيام مسؤولية المنتج أن يكون هناك تسجيل مسبق للرسالة، فإنه لا يجوز للمتهم"CR" أن يدفع بغياب الرقابة. وعلى ذلك، فإن المنتج يتحمل مسؤولية شبه أوتوماتيكية، لا يمكن دفعها إلا بالقوة القاهرة، وهو ما لا يمكن تصوره في هذا المجال.

وحتى يمكن تقدير القيمة الحقيقية لمنطق حكم الدائرة الجنائية، فإنه من المناسب نقل هذا المنطق (الحكم) إلى مجال التليفيزيون، فلنفترض في هذا المجال السمعي البصري، أن مناقشة دارت أمام كاميرا تليفيزيونية أوفي مواجهة "micro Radio phonique" وأن جرائم مماثلة قد ارتكبت، فإذا كان البث مسجلا بصفة مسبقة، فهنا لا تثور أية صعوبة، حيث أنه يمكن ممارسة الرقابة. أما إذا تم البث مباشرة، فإنه لا يمكن ممارسة أية رقابة، وطبقا للفقرة الأولى من م93-3 فإن مدير النشر أو مساعده لا تكون له واقعيا السيطرة على شبكة التلفزيون أو محطة "Radio phonique" ولا يمكن بالتالي إسناد أية تهمة إليهما بخصوص الرسالة المجرمة، لأنها لم تكن محلا لتسجيل سابق، وعكس ذلك، ولأن الفقرة الثانية من المادة السابقة فإن منتج البث

المشرع الفرنسي ورغبة منه في أن لا يفلت المجرم من العقاب أقام مسؤولية المنتج على أساس المسؤولية بالتتابع أو بالتعاقب (responsabilité en cascade).

لقد انتقد الفقه في فرنسا وغيرها حكم مسؤولية المنتج كفاعل أصلي في حالة عدم وجود مدير للنشر، كما انتقد التفسير الحرفي للمادة 93-3 من قانون 1982 للأسباب التالي ذكرها:

– إن التفسير المعطى يحد من نطاق الشرط المنصوص عليه في الفقرة الأولى من م93-3 ويفرغه من مضمونه، إذ بإمكان القاضي أن يتخلص منه بمهارة عن طريق تغيير صاحب المصلحة (المعني) لأن ضرورات عقاب الجرائم المرتكبة عبر الانترنت قد تفرض عليه ذلك.

– يجمع الفقه أن قرائن المسؤولية المنصوص عليها في قانون 1881، وقانون 1982 هي مقابل واجبات الرقابة والإشراف التي تقع على من نسب لهم الاتهام، فيما عدا الفاعلين.

– من غير الجائز من الناحية الأخلاقية أن تكون مسؤولية مدير النشر أخف من مسؤولية المنتج، إذ القرينة على مسؤولية الأول بسيطة، في حين أن القرينة على مسؤولية الثاني لا يمكن دحضها، كونها آلية.

–كما أن حكم محكمة النقض لسنة 1998 لا يتوافق مع التطور التقني.

– إن وظيفة مدير النشر والمنتج المنصوص عليها في م93-3 من قانون 1982 لا تتطابق مع المصطلحات التي ظهرت في مجال الاتصالات، لذا يستحسن تدخل المشرع لوضع نص جديد يتلاءم مع التقنيات الجديدة للاتصال الجماعي أو المشترك، فذلك أفضل من ليّ النصوص السارية.[1]

وحسب حكم محكمة النقض الصادر في 1998/12/08 يسأل عن الأفعال المجرمة كفاعل أصلي في حالة عدم وجود مدير النشر، رغم أن المنتج لم تكن لديه مكنة منع ارتكاب الجريمة بحيث كان البث مباشرا.

بناء عليه فإن نقل حكم محكمة النقض إلى مجال التلفزيون يوضح مدى التناقض الذي شاب نص م93-3، التي ميزت دون مبرر بين مدير النشر أو مساعده، وبين المنتج، عندما أعفت المدير من المسؤولية عن الرسائل غير المشروعة في حالة البث المباشر، لعدم استطاعته مباشرة الرقابة عليها، في حين أن المنتج يسأل عن بث الرسالة غير المشروعة ولو كان البث مباشرا. وهنا يتضح أن المشرع قد أقام نظام المسؤولية بالتتابع في مجال التلفزيون، كما أكد على مسؤولية المنتج بصفة آلية. جميل عبد الباقي، المرجع السابق، ص184 وما بعدها.

[1] الصغير، المرجع السابق، ص ص178-179. يراجع أيضا: حجازي، المرجع السابق، ص149.

وفي قضية أخرى حديثة نسبيا طرح المشكل ذاته بالنسبة للمنتج، حيث أدانته محكمة استئناف "روان"[1] الفرنسية رغم أن البث على الانترنت كان مباشرا، وليس بوسعه ممارسة ثمة رقابة على المتدخلين، غير أن قرارا للمجلس الدستوري –بصدد قضية أخرى- بتاريخ 2011/09/16، نص صراحة على عدم دستورية فرض قرينة قاطعة تقر المسؤولية الجزائية على منشئ(créateur) أو منشط موقع، بسبب محتوى رسالة غير مشروعة منشورة على الموقع، لم يكن يعلم بعدم مشروعيتها قبل وضعها على الخط، مما جعل المحكمة العليا تلغي قرار محكمة الاستئناف وتعيب عليها إدانتها للمنتج "دون البحث عما إذا كان السيد X، يعلم قبل الوضع المباشر على الخط، محتوى الرسالة غير المشروعة، أو في الحالة المعاكسة لم يتصرف كما ينبغي لسحبه بمجرد أن علم بالمحتوى غير المشروع".[2]

رابعا: المسؤولية الجزائية لناقل المعلومات

يفترض في ناقل المعلومات عدم قيامه بمراقبة الرسائل التي تمر خلال الانترنت، ومن ثم لا يسأل عن المحتوى غير المشروع، أما إذا كان ناقل المعلومات يعلم بالمحتوى غير المشروع فإن مسؤوليته تقوم وفقا لما كان يقضي به القضاء بالنسبة لمتعهد الوصول، وتطبيقا لذلك قضت المحكمة الفيدرالية في سويسرا في 1995/02/17، بإدانة الموظف المسؤول عن مكتب البريد بتهمة الاشتراك في مطبوعات مخلة بالحياء، لأنه امتنع عن منع النشاط المحظور رغم أن النيابة العامة كانت قد لفتت انتباهه إلى الممارسات غير المشروعة التي ترتكب على الحاسب الخادم لكشكه.[3]

إن ناقل المعلومات، الذي يقوم في سبيل تسريع عملية اتصال العملاء بشبكة الإنترنت بتخزين نسخة مؤقتة على أجهزته عن صفحات الويب المطلوبة، فإن المادة 13 من التوجيه الأوروبي نصت على عدم إمكانية مساءلته إلا إذا ثبت أنه هو مصدر المضمون المعلوماتي غير المشروع، أو أنه قام بالتغيير فيه أثناء عملية نقله أو تخزينه بشكل أضفى عليه صفة عدم المشروعية، أو أنه تقاعس عن وقف بث المضمون المعلوماتي غير المشروع، رغم تحقق علمه بعدم المشروعية، ووفقا لنص المادة 14 من التوجيه ذاته، والتي اهتمت بتحديد مسؤولية متعهد الإيواء، فإن هذا الأخير غير مسؤول عن

[1] Cour d'appel de Rouen, ch. Corr. 10/10/2010.

[2] Emmanuel Dreyer, nouvelle responsabilité du producteur sur internet, Recueil Dalloz, 17 janvier 2013,p160-163.

[3] بيومي حجازي، المرجع السابق، ص151.

الموقع الإلكتروني ذي المضمون غير المشروع الذي يأويه، إلا إذا لم يتَّخذ الإجراءات اللازمة لوقف بثه بمجرد ثبوت علمه الفعلي بوجود هذه الأنشطة، أو المعلومات غير المشروعة.[1]

خامسا: المسؤولية الجزائية لمتعهد الخدمات

متعهد الخدمات هو ناشر الموقع، وهو صاحب السلطة الحقيقية لمراقبة المحتوى الذي يتم بثه، ويقع على عاتقه بعض الالتزامات منها إخطار النائب العام بخدمة الاتصال السمعية البصرية، وكذا الإيداع القانوني، كما يلتزم بتعيين شخص طبيعي كمدير للنشر، كي يتحمل المسؤولية الجزائية عن مضمون الخدمة،[2] ومن التزاماته أيضا حسن القيام بالخدمة المعلوماتية، ومراقبة محتوى الرسائل التي تصل إليه، ليقرر إن كانت مشروعة أم لا.

يجوز لمزود الخدمات أن يقوم بأكثر من وظيفة، كتمويل المعلومات، ولعب دور متعهد الوصول...مما يرتب عليه المسؤولية المدنية والجزائية عن المعلومات الكاذبة أو الناقصة أو المضللة أو الفاضحة التي قام بإعدادها ونشرها على موقعه؛ فهو يشبه مدير النشر في جرائم الصحافة.[3]

سادسا: المسؤولية الجزائية لمورد المعلومات

مورد المعلومات هو الذي يقوم بالاختيار ثم التجميع والتوريد للمادة المعلوماتية حتى تصل إلى الجمهور على الشبكة، حيث يسيطر على المعلومات سيطرة كاملة، وكنتيجة لذلك يلتزم باحترام أحكام القانون، سيما المتعلقة بالنظام العام، لذلك يعاقب جزائيا إذا ثبت قيامه ببث أو تسجيل صور مخلة بالآداب العامة بهدف نشرها (م227-22 ق ع ف)، وإذا كان هو من قام بتصنيع هذه الصور يعاقب حسب (م227-22 ق ع ف) المتعلقة بتسهيل أو محاولة تسهيل إفساد

---

[1] أحمد فرح، المرجع السابق، ص354.

[2] Le TGI de Montpellier a relaxé le directeur de la publication d'un blog qui avait agi promptement pour retirer un commentaire diffamatoire envers un fonctionnaire, par un jugement du 5 février 2015.
Dans cette affaire, il était reproché au président de l'Académie des arts et des sciences de Carcassonne d'avoir hébergé dans les rubriques « coups de gueule » et « notes récentes » du blog de celle-ci un commentaire qui attribue à un fonctionnaire municipal des procédés rappelant « les autodafés d'Allemagne ». Si les termes sont sans conteste diffamatoires pour le tribunal, ce dernier rappelle cependant que le directeur de la publication peut s'exonérer de sa responsabilité s'il ne connaissait pas le contenu de ce message avant sa mise en ligne ou s'il établit qu'il l'a retiré une fois informé de sa nature litigieuse. Celui-ci avait exercé son contrôle sur les milliers de réactions qu'avait suscités la parution d'un article du Midi libre dénonçant la mise à la décharge de milliers de livres de la bibliothèque municipale. Mais le commentaire en cause lui avait échappé. Toutefois, dès qu'il avait été saisi de la demande de retrait par la personne incriminée, il avait retiré du message le terme « allemand », enlevant ainsi toute imputation susceptible de porter atteinte à sa réputation. Voir le site : légalis.net.

3 بيومي حجازي، المرجع السابق، ص152.

قاصر، كما أن مورد المعلومات قد يقع تحت م321-1 ق ع ف إذا قام بجمع الصور لأنه أصبح حائزا لمعلومات متحصلة من جنحة، مما يشكل جريمة إخفاء.[1]

ولم يفت القضاء أيضا، تحديد أسس مساءلة مورد المعلومات على شبكة الإنترنت، فقد عدت محكمة صلح (بوتوه) في قرارها الصادر في 28 سبتمبر1999 أن مورد المعلومات، ونظرا لطبيعة الخدمة التي يؤديها، هو المسؤول الأول عن بث المعلومات الإلكترونية غير المشروعة عبر الشبكة، وقامت بمساءلته جنبا إلى جنب مع متعهد الإيواء بوصفهم مسؤولين عن تقديم الخدمة المعلوماتية، وقد أكدت محكمة استئناف فرساي في قرارها الصادر بتاريخ 8 جوان 2000 على أن قيام مسؤولية مورد المضمون المعلوماتي غير المشروع يجب أن لا يكون سببا لاستبعاد مسؤولية متعهد الإيواء في حال ثبوت خطئه. [2]

سابعا:المسؤولية الجزائية لمؤلف الرسالة

مؤلف الرسالة هو المسؤول الأول عن أي معلومات غير مشروعة تتضمنها الرسالة، وفقا للقواعد العامة التي تقيم مسؤولية مؤلف الرسالة في جريمة السب والقذف بطريق النشر بوصفه شريكا في الجريمة وليس الفاعل الأصلي حسب قانون الصحافة الفرنسي، ويبرر الفقه ذلك بأن مؤلف الرسالة غالبا ما يوقع على رسالته باسم مستعار، ومن ثم يصعب تحديد عنوانه على الانترنت، ومن ناحية أخرى لتمكين الضحية البحث عن مسؤولين آخرين أقل تعسرا من مؤلف الرسالة، ولذا ترفع الدعاوى على الناشرين بوصفهم فاعلين أصليين في هذه الجرائم.[3]

يلحق بمسؤولية مؤلف الرسالة، مسؤولية مورد الرسائل الفنية، وهو الذي يقوم بإدخال المعلومات في الخط، من غير أن يتدخل في الخدمة أو يمارس رقابة على المعلومات التي تمر في أية لحظة، ولذا لا يجوز مساءلته جزائيا عن المحتوى غير المشروع الذي يعبر الشبكة.[4]

بالنسبة للمشرع الجزائري فقد تناولت بعض النصوص موضوع مقدمي الخدمات والالتزامات الملقاة على عاتقهم، أهمها القانون رقم 09-04 المتعلق بتكنولوجيا الإعلام والاتصال،

---

[1] بيومي حجازي، المرجع السابق، ص154.

[2] محمد حسين منصور، المرجع السابق، ص180.

[3] بيومي حجازي، المرجع السابق، ص155.

[4] المرجع نفسه، ص157.

وقد جاء في م2/د منه تعريف مقدمي الخدمات،[1] كما بينت المواد 10، 11، 12 من القانون السابق التزامات مقدمي الخدمات، وتتمثل حسب م10 من القانون السابق، في مساعدة السلطات المكلفة بالتحريات القضائية لجمع وتسجيل المعطيات المتعلقة بمحتوى الاتصالات في حينها، وبوضع المعطيات التي يتعين عليهم حفظها تحت تصرف السلطات المذكورة، ويجب عليهم كتمان سرية العمليات التي ينجزونها بطلب من المحققين، وكذا المعلومات المتصلة بها تحت طائلة العقوبات المقررة لإفشاء أسرار التحري والتحقيق. لم يبين المشرع العقوبة المقررة كجزاء للإخلال بواجب كتمان أسرار التحري والتحقيق، في هذه المادة، لذا يجوز أن يطبق بشأنهم نص م301 ق ع كونهم مؤتمنون بحكم الوظيفة على الأسرار.

كما ألزمت م11 من القانون رقم 09-04 سالف الذكر مقدمي الخدمات بحفظ المعطيات المتعلقة بحركة السير لمدة سنة واحدة ابتداء من تاريخ التسجيل، تحت طائلة العقوبات الإدارية، وكذا العقوبة الجزائية المقدرة بالحبس من ستة أشهر إلى خمس سنوات، والغرامة من 50.000 دج إلى 500.000 دج إذا كان مزود الخدمة شخصا طبيعيا، والغرامة وفقا للقواعد العامة المقررة في قانون العقوبات إذا كان مزود الخدمة شخصا معنويا أي 2500.000 دج.

واشترط المشرع الجزائري لقيام مسؤولية مزودي الخدمة الجزائية، أن يؤدي الفعل الإجرامي المتمثل في عدم احترام مزودي الخدمات للالتزامات المنصوص عليها في م11 من القانون رقم 09-04، إلى تحقق نتيجة ضارة وهي عرقلة حسن سير التحريات القضائية.

كما ألزمت م12 من القانون رقم 09-04 مزودي خدمات الانترنت بالتزامات خاصة، تتمثل في التدخل الفوري لسحب المحتويات غير المشروعة بمجرد العلم بذلك، وتخزينها، أو جعل الدخول إليها غير ممكن، وكذا وضع ترتيبات تقنية لحصر إمكانية الدخول إلى الموزعات التي تحوي معلومات مخالفة للنظام العام أو الآداب العامة، وإخبار المشتركين لديهم بوجودها. غير أن هذه المادة لم تبين العقوبة الجزائية المترتبة عن الإخلال بالالتزامات التي أوردتها، مما يجعل الرجوع إلى القواعد العامة أمرا ضروريا.

[1] عرفت م2/د من القانون 04/09 مقدمي الخدمات بأنهم: "1- أي كيان عام أو خاص يقدم لمستعملي خدماته القدرة على الاتصال بواسطة منظومة معلوماتية و/أو نظام للاتصالات، 2- وأي كيان آخر يقوم بمعالجة أو تخزين معطيات معلوماتية لفائدة خدمة الاتصال المذكورة أو لمستعمليها".

كما أن م14 من المرسوم التنفيذي رقم 98-257،[1] ذكرت التزامات مقدم خدمات الانترنت خلال ممارسة نشاطه.

كما أن المادتين 70 و71 من القانون 15-04 المتعلق بالتوقيع والتصديق الإلكترونيين عاقبتا على إخلال مؤدي خدمات التصديق الإلكتروني بالالتزامات التي فرضها القانون المذكور عليهم.

إن الخدمات الوسيطة في التجارة الإلكترونية شديدة الشبه بالخدمات الوسيطة المتعلقة بالتجارة التقليدية، فهناك شركات نقل تساعد التجار في نقل بضائعهم، وهناك ناقل الخدمة الذي يمكّن المستخدم من الاتصال بالشبكة ونقل المعلومات إليها، وفي التجارة الإلكترونية هنالك مورد المعلومات، وفي التجارة التقليدية هناك تاجر الجملة الذي يورد بضاعته لتاجر التجزئة، كذلك هنالك متعهدو الإيواء أو التخزين في التجارة الإلكترونية، وهنالك من يقوم بالتخزين في التجارة التقليدية، ومما سبق فإن تحديد المسؤولية الجزائية لمقدمي الخدمات الوسيطة في شبكة الانترنت يسهم في إضفاء نوع من الحماية للتجارة الإلكترونية ويدعم ثقة المستهلكين فيها.[2]

[1] مؤرخ في 25 غشت 1998، يضبط ويحدد شروط وكيفيات إقامة خدمات "انترنت" واستغلالها، المعدل بموجب المرسوم التنفيذي رقم 2000-307، المؤرخ في 2000/10/14.

[2] د. عبد الفتاح بيومي حجازي، الجرائم المستحدثة في نطاق تكنولوجيا الاتصالات الحديثة، منشأة المعارف، الإسكندرية، مصر 2009، ص120.

الباب الثاني: القواعد الإجرائية المتعلقة بالتجارة الإلكترونية.

إن الحماية الجزائية للتجارة الإلكترونية لا يجب أن تقتصر فقط على الجانب الموضوعي، بل ينبغي أن تمتد لتشمل الجانب الإجرائي أيضا، فهذان الجانبان هما بمثابة جناحي الحماية الجزائية للتجارة الإلكترونية، لا غنى لها عنهما، بل قد لا نكون مغالين عند القول بأن الجانب الإجرائي أكثر أهمية من الجانب الموضوعي، لأنه يقف على المشكلات الواقعية المتعلقة بهذه التجارة ويسعى إلى حلها عمليا.

يتطرق هذا الباب إلى جملة من النقاط الهامة المتعلقة بالقواعد الإجرائية في مجال التجارة الإلكترونية، ليحاول الإجابة عن جملة من التساؤلات، لعل من أبرزها التساؤل التالي: هل هذه الجرائم تقتضي قواعد إجرائية خاصة ومتميزة عن القواعد الإجرائية العامة للكشف عن مرتكبيها والتحقيق معهم ومحاكمتهم ثم معاقبتهم؟ أم أن القواعد الإجرائية العامة وحدها كافية؟ كيف يمكن التعامل الإجرائي مع مثل هذه الجرائم المستحدثة لكشف مرتكبيها دون المساس بالضمانات القانونية التي يمنحها القانون للأشخاص؟ أي دون المساس بحقوق الأفراد؟ وهل تستطيع كل دولة منفردة محاربة الجرائم الإلكترونية أم وجب التعاون الدولي في ما بين الدول؟ وإذا كانت الإجابة بضرورة التعاون، فما هي أشكال هذا التعاون؟ وما هي المعوقات التي تقف أمامه؟ وما سبل تعزيزه؟

للإجابة عن هذه التساؤلات وغيرها يقسم هذا الباب إلى فصلين، يتناول الفصل الأول الحماية الجزائية الإجرائية للتجارة الإلكترونية في التشريعات الوطنية، ويتطرق الفصل الثاني إلى التعاون الدولي في مجال مكافحة جرائم التجارة الإلكترونية.

الفصل الأول: الحماية الإجرائية الوطنية للتجارة الإلكترونية.

نتيجة تنامي حجم التجارة الإلكترونية، إذ أصبحت واقعا مفروضا يجب التعامل معه، وعدم التغاضي عنه، وما صاحب هذه التجارة من اعتداءات مختلفة عليها، بادرت مختلف الدول إلى إقرار تدابير فنية وقانونية لحماية التجارة الإلكترونية، فمنها من عدلت قوانينها لتتناسب مع طبيعة الجرائم الإلكترونية، ومنها من أصدرت قوانين جديدة لمجابهة هذه الجرائم المستحدثة، ومن ذلك القواعد القانونية الإجرائية، التي تهدف إلى تحقيق حماية إجرائية للتجارة الإلكترونية سواء قبل مرحلة المحاكمة (المبحث الأول)، أو أثناء مرحلة المحاكمة (المبحث الثاني).

المبحث الأول: الحماية الجزائية للتجارة الإلكترونية من خلال الإجراءات الجزائية السابقة على المحاكمة.

لحماية إجرائية مثلى للتجارة الإلكترونية، لا بد من مراعاة اعتبارين هامين وهما: الحصول على الدليل لإدانة مرتكبي الجرائم، ومراعاة مبدأ شرعية هذا الدليل والذي غالبا ما يكون إلكترونيا، باعتبار أن هذه الجرائم تقع في البيئة الإلكترونية، وهذا يتطلب بدوره جملة من الأمور لعل من أهمها أن يكون القائمون على جمع هذه الأدلة على درجة عالية من الكفاءة والخبرة والدراية بخبايا التعاملات الإلكترونية، وتلاعبات مجرمي المعلوماتية وحيلهم، بحيث تُتبع وسائل معينة للحصول على الدليل الإلكتروني مع المحافظة على حقوق الأشخاص، ودون المساس بالمبادئ المكرسة وطنيا ودوليا، وأهمها مبدأ أو قرينة أو أصل البراءة.

يعالج هذا المبحث من خلال التطرق إلى الضبط والتحقيق في مجال التجارة الإلكترونية، وإجراءات الحصول على الدليل الإلكتروني.

المطلب الأول: الضبط في مجال الجرائم المتصلة بالتجارة الإلكترونية.

يتم معالجة هذا المطلب من خلال التطرق إلى الضبط الإداري، ودوره في الوقاية من الجرائم (الفرع الأول)، ثم إلى الضبط القضائي (الفرع الثاني).

الفرع الأول: الضبط الإداري ودوره في الوقاية من الجرائم الواقعة على التجارة الإلكترونية.

يتم التطرق أولا إلى مفهوم الضبط الإداري، ثم إلى الضبط الإداري الاقتصادي ودوره في حماية التجارة الإلكترونية.

أولا: مفهوم الضبط الإداري.

يميز الفقه بين نوعين من الضبط: الضبط القضائي والضبط الإداري، ويختلف العمل القضائي عن العمل الإداري، فالعمل القضائي هو العمل الذي تقوم به هيئة قضائية، والعمل الإداري تتولاه الإدارة، كما أن القاضي يطبق القانون، أما الإدارة فهي تعمل وفق القانون،[1] فالضبط القضائي يمارس تحت السلطة الإدارية (المتمثل في وزارة الداخلية بالنسبة للشرطة)، وهدفه الوقاية من الجرائم.[2]

يقصد بالضبط القضائي الإجراءات التي تتخذها سلطة الضبطية القضائية في التحري عن الجرائم بعد حدوثها، في سبيل القبض على مرتكبي هاته الجرائم، وجمع الأدلة اللازمة للتحقيق، وإقامة الدعوى لمحاكمة المتهمين، وإنزال العقوبة على من تثبت إدانته وفق إجراءات غايتها علاج آثار الجرائم وردع مرتكبيها بعد حدوثها؛ فالضبط القضائي لا يتحرك إلا بعد وقوع انتهاك للنظام العام، لمعالجة آثار هذا الانتهاك، على خلاف الضبط الإداري الهادف إلى وقاية النظام العام من الانتهاك قبل وقوعه.[3]

وينقسم الضبط الإداري إلى ضبط إداري عام، وهدفه حماية النظام العام للدولة، وتحقيق الأمن العام والصحة العامة والسكينة العامة؛ وضبط إداري خاص غايته حماية نظام قانون خاص، كحماية الطرق والحدائق العامة والأمن الصناعي وغير ذلك، وبناء عليه، يعتبر من قبيل الضبط

---

[1] السقا، المرجع السابق، ص372.

[2] Jacques Leroy, procédure pénale, librairie générale de droit et de jurisprudence, Lextenso édition, 2009, paris cedex, p76.

[3] د. عبد الغني بسيوني عبد الله، النظرية العامة في القانون الإداري، منشأة المعارف بالإسكندرية، مصر 2003، ص391.

الإداري الخاص حماية التجارة الإلكترونية وغيرها من المواضيع المتصلة بها، كحماية التوقيع الإلكتروني، وبطاقات الائتمان وحقوق المؤلف عبر الانترنت... من مختلف الاعتداءات التي يمكن أن تطالها؛ فهو ضبط وقائي هدفه منع وقوع الجريمة، فيدخل بذلك في الأعمال الإدارية.[1]

تقوم الشرطة في نطاق القواعد العامة بأعمالها الإدارية من خلال الأعمال التنظيمية التي تصدرها الإدارة تنفيذا للقوانين، إذ تقوم بتنفيذ الأحكام الصادرة ضد المتهمين وإيداعهم السجون، وتنفيذ النظام القانوني المعمول به في السجن، كما تقوم بمنع بعض الأشخاص من السفر إلى الخارج كإجراء وقائي في حدود اختصاصاتها.[2]

ومن أعمال الضبط الإداري ما تقوم به مصالح الدرك الوطني ببلادنا، المختصة بالجرائم المعلوماتية، أو ما يسمون بدركيي الانترنت من حرص ويقظة وتأهب وعمل على استباق الإجرام المعلوماتي حتى قبل وقوعه.[3]

في الولايات المتحدة الأمريكية تتبع الشرطة أسلوبا وقائيا، يسمى (الطعم الخادع)، حيث يرتدي رجال الشرطة أحيانا زيا بغية (الخداع)، يكون في عدة صور منها: رجل أعمال سائح، أجنبي عن المدينة...لجذب المجرم، حيث يعتقد هذا الأخير أنه قد عثر على (صيد سهل)، فيقوم المجرم بالتصرف مع هذا الشخص (رجل الشرطة) حسب الجريمة التي يود ارتكابها، فقد يجد المجرم فرصته في استدراجه نحو سرقة بطاقته الائتمانية مثلا أو معرفة رقمها أو غير ذلك، وبهذه الطريقة يستدرج رجل الشرطة المجرم حتى يوقعه في الشرَك، أو على الأقل يكون للشرطة معلومات حول بعض المجرمين، تحتاج إليها عند وقوع جرائم حقيقية،[4] كما تقوم الهيئات المختصة في بعض الدول بأنشطة خادعة على الانترنت، كعرض صور فتيات غير حقيقية، لتلقي طلبات المهووسين بارتكاب جرائم الجنس على الأطفال، وتتبعهم تمهيدا لاتخاذ الإجراءات الكفيلة بردعهم.

غير أن ذلك لا يعني أن تقوم الشرطة أو الجهات المختصة بالتحريض على ارتكاب الجريمة لإلقاء القبض على أصحابها، فذلك مسلك منتقد، ويتنافى مع مبدأ أصل أو قرينة البراءة،

---

[1] د. عبد الغني بسيوني عبد الله، المرجع السابق، ص392. ويراجع أيضا: السقا، المرجع السابق، ص378.

[2] السقا، المرجع نفسه، ص379.

[3] كرود عبد الحميد، التسول، النصب والاحتيال عبر الانترنت، مجلة الدركي، العدد16، نوفمبر 2008، ص49.

[4] السقا، المرجع السابق، ص380.

وينتج عنه بطلان الدليل المبني على هذا الإجراء المعيب، ومن تطبيقات ذلك ما حكمت به محكمة باريس بإلغائها "إبطالها" تقريرا لتحقيق أولي للضبطية القضائية، ليس فقط لأن التنصت على المكالمات الهاتفية لم يتم وفقا للإجراءات القانونية الصحيحة ومن ذلك الحصول على ترخيص من قاضي التحقيق، بل وأيضا لأن الشرطة دفعت بالمتهم طيلة شهرين على ارتكاب الجريمة عن طريق تحريضه على ذلك.[1]

ثانيا: الضبط الإداري الاقتصادي ودوره في حماية التجارة الإلكترونية.

الأمن الاقتصادي جزء من أمن الدولة، وهو جزء هام للغاية، يجب المحافظة عليه من قبل الشرطة وغيرها، والتصدي لكافة أنواع الإجرام الاقتصادي والمالي ومنها الاعتداءات الواقعة على التجارة الإلكترونية كتخريب المعلومات وإساءة استخدامها، وتزوير العلامات التجارية وبطاقات الائتمان...[2] ويمتد أمن الدولة الاقتصادي ليشمل أيضا أمن الفرد الاقتصادي.

ولا شك أن حماية التجارة الإلكترونية يحقق الأمن الاقتصادي للدولة والفرد معا؛ فالجرائم الواقعة على التجارة الإلكترونية أخطر بكثير – في نظر الكثير من الفقه – من جرائم التزييف وتزوير العملة واختلاس المال العام، وجرائم البورصات، والرشوة واستغلال النفوذ... ومحاربة هذه الجرائم كلها يرمي إلى تحقيق الأمن الاقتصادي.[3]

ومن الإجراءات المتبعة في مجال الضبط الإداري لجرائم الحاسب الآلي، تأمين شبكات المعلومات من الهجوم والاختراق عن طريق مجموعة من الأمور الفنية، ومجموعة من الإجراءات لتأمين الحاسب الآلي، أو تأمين التشغيل، أو تأمين الموقع، أو تأمين نظم المعلومات.

ولا شك أن تأمين الحاسب الآلي يساعد كثيرا في تأمين وحماية التجارة الإلكترونية، باعتبار الحاسب الآلي أحد أهم الوسائل الأكثر استعمالا في التجارة الإلكترونية.

---

[1] Jacques Leroy, op cit, p77.

[2] مختار شبيلي، الإجرام الاقتصادي والمالي الدولي وسبل مكافحته، ط2 دار هومة، الجزائر 2012، ص57.

[3] السقا، المرجع السابق، ص373.

هناك بعض الأساليب التي يجوز أن تتخذها الشرطة أو أعوان الضبط الاقتصادي لتأمين التجارة الإلكترونية، كتفتيش المحلات ومقاهي الانترنت، ومراقبة مختلف التبادلات الإلكترونية، والتأكد من سلامة بطاقات الائتمان، على أن يتم هذا الأمر باحترافية تامة، وفي إطار احترام القانون، صونا للأشخاص، وحفاظا على سلامة الإجراءات المتبعة.

وعلى مستوى البنوك ومؤسسات إصدار البطاقات تم إرساء نظام جديد للتعامل فيما بينها، وإعداد بنية تحتية لنظم تشفير الرسائل والمعاملات الإلكترونية، وتحويل الأموال عبر شبكة الانترنت لتأمين أنظمة التعامل ببطاقات الائتمان، كما تم تصميم عدة برامج للحيلولة دون وقوع الاعتداءات على البطاقات، وغالب هذه البرامج طورت على يد البنوك.[1]

الفرع الثاني: الضبط القضائي ودوره في التصدي للجرائم الواقعة على التجارة الإلكترونية.

تمر الخصومة الجزائية بعدة مراحل قبل أن تصل إلى المحكمة، أولها مرحلة الضبط القضائي، وهي مرحلة تمهيدية لضبط الجريمة وجمع الأدلة، والمعلومات اللازمة عنها، وبعد ذلك تمر الخصومة بمرحلة ثانية يطلق عليها مرحلة التحقيق الابتدائي، يتولاها في الجزائر وفرنسا قاضي التحقيق، أما في مصر فالتحقيق من صلاحيات النيابة العامة، وتختلف مهمة الضبط القضائي عن مهمة التحقيق الابتدائي كون الأولى من طبيعة بوليسية، وتعد بمثابة مرحلة تحضيرية للتحقيق الابتدائي الذي يقوم به قاضي التحقيق، وهو من طبيعة قضائية، ويجري بعد تأكد وقوع الجريمة فعلا، وهذا الاختلاف ينتج عنه اختلاف آخر في الضمانات التي يتطلبها القانون في كل منهما، فالتحقيق الأولي كونه من طبيعة بوليسية أحاطه القانون بضمانات أكبر، صيانة للحريات الفردية وحماية لها.[2]

وبصفة عامة فإن رجال الضبطية القضائية ينبغي عليهم التقيد بالإجراءات المشروعة والابتعاد عن كل الإجراءات غير المشروعة، حتى لا تكون معيبة بما يبطلها، ومثال ذلك استراق السمع والمشاهدات التي يختلسها رجال الضبطية القضائية من خلال ثقوب أبواب المساكن، لما في هذا من مساس بحرمة المساكن ومنافاة الآداب.

---

[1] السقا، المرجع السابق، ص389.

[2] العربي بلحاج، أبحاث ومذكرات في القانون والفقه الإسلامي، ج1، د م ج، بن عكنون، الجزائر 1996، ص ص309-310.

ويعد من الإجراءات الباطلة تحريض رجال الضبطية القضائية للآخرين على اقتراف جريمة، كأن يتخفى ضابط شرطة قضائية في زي أحد العوام ويعرض رشوة على الموظف العام للإيقاع به، وليس لكشفه باعتباره مشبوها، فالعبرة ألا يكون التحريض هو الدافع على ارتكاب الجريمة.[1]

تواجه الضبطية القضائية صعوبات كثيرة عندما تتصدى للجرائم الإلكترونية، تكمن خاصة في الحصول على الدليل عن أفعال التعدي، بحيث أن مجرمي المعلوماتية يحيطون أنفسهم بسياج أمني متمثل في وسائل تقنية متطورة حتى لا يتمكن رجال الضبطية القضائية من اقتفاء أثرهم، ويزيد من صعوبة الكشف عن الجرائم الإلكترونية أن كثيرا من المجني عليهم يحجمون عن التبليغ عن هذا النوع من الجرائم لاعتبارات مختلفة منها الخوف على السمعة.[2]

عموما إن معظم التشريعات المقارنة قد أجازت التحريات التي لا تتعلق بحرمة الحياة الخاصة، فرجال الضبطية القضائية لهم أن يقوموا بالتحريات المختلفة التي ترد على بيانات الأفراد المشتبه فيهم، طالما أن تجميع تلك البيانات لا يتضمن اعتداء على حرمة الحياة الخاصة.

ولا يقتصر الحق في الحياة الخاصة على المعلومات المتعلقة بوجود الشخص في مكان خاص، بل يمتد ليشمل أيضا البيانات المتعلقة بتواجد الشخص في مكان عام طالما أنها معلومات شخصية، يحرص صاحبها على عدم نشرها،[3] ولا تدخل أسرار البنك ضمن مجال الحياة الخاصة، بل ضمن نطاق الأسرار التجارية كأصل عام، لذا يجوز كشف سرية الحسابات المصرفية بمقتضى أمر أو إذن قضائي في الحالات المحددة قانونا.[4]

يجوز لرجال الضبط القضائي دخول الأماكن العامة دون الحصول على إذن مسبق، كما يجوز لهم أن يدخلوا إليها كما يدخل أي شخص عادي، ولهم في ذلك جميع ما يتمتع به هذا الرجل العادي، ولكن لا يجوز لهم فتح الأشياء المغلقة الموجودة في المحلات العامة، وعليه لا يجوز لرجال

---

[1] د. عبد الفتاح بيومي حجازي، الجوانب الإجرائية لأعمال التحقيق الابتدائي في الجرائم المعلوماتية، دار النهضة العربية، القاهرة 2009، ص157.

[2] شيماء عبد الغني، المرجع السابق، ص193.

[3] المرجع نفسه، ص194.

تطبيقا لذلك قضي في كندا أنه لا يجوز التقاط صورة امرأة دون رضاها ولو كان ذلك في مكان عام، غير أنه إذا كان المتهم يتزعم مظاهرة فإنه يجوز لرجال الضبط تصويره في هذا الوضع، لأنه لا يحرص على ضمان حقه في الصورة في هذه الحالة، كما أن البنوك تضع كاميرات لتصوير المترددين عليها، ولا يعد ذلك اعتداء على حرمة الحياة الخاصة. المرجع نفسه، ص194.

[4] المرجع نفسه، ص197.

الضبطية القضائية دخول مقاهي الانترنت، وفتح الحاسب الآلي المغلق، أو الجلوس إلى حاسب مفتوح والبحث فيه، اللهم إلا إذا رأوا جهازا مفتوحا وبه مخالفات واضحة، فهنا تقوم حالة التلبس التي تجيز لهم ضبط وتفتيش هذه الأجهزة، غير أن رجال الضبط القضائي إذا دخلوا بصفتهم أشخاصا عاديين، فيحق لهم استعمال جهاز الحاسب الآلي كما يستعمله الأفراد العاديون، فإن اكتشفوا جريمة، كاستعمال برامج مقلدة، فإن من حقهم اتخاذ إجراءات الضبط، وتكون في هذه الحالة متفقة مع صحيح القانون.[1]

غير أن رجال الضبط القضائي لا يجوز لهم القيام بإجراءات التفتيش إلا بعد الحصول على إذن بذلك، فلا يجوز لهم فتح أجهزة الإعلام الآلي لمعرفة المواقع التي استعملها شخص جالس على الجهاز، لكي يميز من بينها ما يعتبر منافيا للآداب وما لا يعتبر كذلك، كما لا يجوز فتح ملف مخزن بالجهاز والإطلاع عليه، فهذا العمل لا يدخل في إطار سلطة الضبطية القضائية في القيام بالتحريات، وإنما يعد من قبيل التفتيش الذي يحتاج إلى إذن، أو حالة تلبس، كما لا يجوز التجول في الأجزاء الخاصة للأشخاص على الحاسب الآلي أو على شبكة الانترنت، أو الإطلاع عليها، فلا يجوز اقتحام البريد الإلكتروني للأشخاص، ويتعين فقط البقاء في المواضيع المتاحة للجمهور.[2]

عموما فإن حدود صلاحيات رجال الضبط القضائي هي حرمة الحياة الخاصة للأفراد التي يجب عدم تجاوزها، وهذه مسألة موضوعية متروكة للقضاء، فقد قضي بأن معرفة رقم الهاتف ورقم الاتصال بأشخاص معينين دون تسجيل المكالمة أو اعتراض المراسلة الإلكترونية لا يعتبر مساسا بحرمة الحياة الخاصة،[3] فالأصل أن طبيعة إجراءات الاستدلال لا ينبغي أن تنطوي على مساس بالحرية الشخصية، إذ يفترض فيها أنها تقتصر على مجرد جمع المعلومات حول الجريمة المرتكبة، ولكن الواقع غير ذلك، خاصة في دول العالم الثالث، فهي تنطوي أحيانا على مساس بالحريات المكفولة للأفراد سواء في الدساتير أو المواثيق الدولية لحقوق الإنسان.[4]

---

[1] شيماء عبد الغني، المرجع السابق، ص200.

[2] المرجع نفسه، ص201.

[3] المرجع نفسه، ص201.

[4] د. أسامة عبد الله قليد، الوسيط في شرح قانون الإجراءات الجنائية المصري، دار النهضة العربية، القاهرة 2003، ص103.

في القانون الجزائري، وحسب نص م14 من ق إ ج فإن الضبط القضائي يشمل ضباط الشرطة القضائية، أعوان الضبطية القضائية، الموظفين والأعوان المنوط بهم بعض أعمال الضبط القضائي؛ وذكرت م15 ق إ ج من هم الأشخاص الذين يتمتعون بصفة ضباط الشرطة القضائية، أما م19 من القانون ذاته فقد تطرقت إلى أعوان الضبط القضائي، كما تطرقت م21 من ق إ ج إلى فئة الموظفين والأعوان الذين يكلفون ببعض مهام الضبط القضائي، كما أشارت م27 من ق إ ج إلى فئات أخرى لهم صفة الضبطية القضائية بموجب قوانين خاصة، كأعوان الجمارك، وأعوان الضرائب والمستخدمين المنتمين إلى الأسلاك الخاصة بالمراقبة وغيرها.

طبقا لنص م1/16 ق إ ج يتحدد الاختصاص المكاني لرجال الضبطية القضائية بحدود الدائرة التي يباشرون فيها وظائفهم المعتادة، وفي المدن المقسمة إلى عدة دوائر للشرطة يمتد اختصاص محافظي و ضباط الشرطة إلى كافة المجموعة السكنية للمدينة (م5/16)، ويكون اختصاص ضابط الشرطة القضائية وطنيا إذا تعلقت الأبحاث والمعاينات بجرائم المخدرات... **والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات**... مهما كانت الجهة التي ينتمي إليها ضابط الشرطة القضائية (م7/16 ق ا ج).

كما أجازت م16 مكرر ق إ ج تمديد الاختصاص لضباط الشرطة القضائية وأعوانهم (ما لم يعترض على ذلك وكيل الجمهورية المختص بعد إخباره) إلى كامل التراب الوطني للقيام بعمليات مراقبة الأشخاص الذين يوجد ضدهم مبرر يحمل على الاشتباه فيهم بارتكاب إحدى الجرائم المتعلقة بالمخدرات أو المساس بأنظمة المعطيات أو تبييض الأموال أو جرائم الإرهاب أو الجرائم المنظمة عبر الحدود الوطنية أو الجرائم المتعلقة بالتشريع الخاص بالصرف، ومراقبة كذلك وجهة أو نقل أشياء أو أموال أو متحصلات هذه الجرائم أو قد تستعمل في ارتكابها.

الفرع الثالث: دور شرطة الانترنت في حماية التجارة الإلكترونية

تلعب شرطة الانترنت والضبطية القضائية المختصة بالجرائم الإلكترونية دورا رئيسا في حماية التجارة الإلكترونية، لما تتمتع به من إمكانات ومؤهلات لا تتوافر في غيرها، وقد دأبت بعض الدول منذ إحساسها بخطر الجرائم الإلكترونية على إيجاد هذه الآليات الكفيلة للتصدي لهذه الجرائم، ومن ذلك:

الولايات المتحدة الأمريكية: تعتبر الولايات المتحدة الأمريكية من أوائل الدول التي سبقت إلى إحداث شرطة لمحاربة جرائم الانترنت، ففي عام 1978 تم إنشاء شرطة الانترنت والتي تهدف لمحاربة الأنشطة غير المشروعة على هذه الشبكة، وتم وضع عدة أقسام ووحدات شرطية لمواجهة هذا الإجرام والحد من خسائره ومنها:[1]

أ- مكتب رئيس التكنولوجيا: وهو مكتب مفوض مباشرة من مكتب مدير التحقيقات الفيدرالية الأمريكي، لتسيير مختلف المشروعات التكنولوجية وملاحقة مرتكبي الجرائم الواقعة في ذلك المجال، كما تم إنشاء وكالة تابعة لمكتب التحقيقات الفيدرالي إلى جانب المركز الوطني لحماية البنية التحتية، مهمتها التنسيق في مكافحة القرصنة المعلوماتية، ويعتبر مكتب التحقيقات الفيدرالي في حد ذاته الجهاز القيادي لمواجهة الإرهاب عبر الانترنت.

ب- قسم جرائم الحاسبات الآلية وجرائم حقوق الملكية الفكرية: تم إنشاء هذا القسم سنة 1991، ويختص بالكشف عن جرائم الحاسب الآلي وحقوق الملكية الفكرية وملاحقة مرتكبيها.

المركز الوطني لحماية البنية التحتية: وهو جهاز تابع للمباحث الفيدرالية الأمريكية، تم إنشاؤه في 1998/2/28، والذي يتقاسم مهامه مع وزارة الدفاع.

بالإضافة إلى ذلك فقد تم تأسيس مركز لتلقي شكاوى الاحتيال عبر الانترنت من طرف مكتب التحقيقات الفيدرالي، وإلى جانب تلك الأقسام والمراكز، هناك وحدة متخصصة تابعة لقسم العدالة الأمريكي، مكلفة بمكافحة الإجرام المعلوماتي، تتكون من خبراء في تقنيات الحاسب الآلي والانترنت، ومن خبراء قانونيين أيضا بغية إحداث تكامل بين ما هو فني صرف وما هو قانوني.

فرنسا: تعتبر فرنسا من الدول الأولى التي أسهمت بشكل فعال في مكافحة جرائم الاعتداء على التجارة الإلكترونية بشكل خاص، والجرائم المعلوماتية بصفة عامة، من خلال شرطة متخصصة للانترنت عن طريق:

أ- المكتب المركزي لمكافحة الإجرام المرتبط بتكنولوجيا المعلومات والاتصال (OCLCTIC)[2] ولقد تم إنشاؤه بموجب مرسوم وزاري رقم 2000-405 على مستوى الإدارة المركزية للشرطة القضائية

[1] أيمن رمضان، المرجع السابق، ص427.

[2] Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication.

التابعة لوزارة الداخلية، ومهمته تركيز (centraliser) المعلومات المتعلقة بالجرائم الإلكترونية،[1] ويختص هذا المكتب وفقا للمادة الثالثة من المرسوم المذكور بالاختصاصات التالية:

تنشيط ملاحقة الجرائم المتعلقة بتكنولوجيا المعلومات، واتخاذ إجراءات الضبط والتفتيش، وفحص وحدات الحاسب الآلي على اختلافها كالأقراص الصلبة والمعطيات المتحصلة من الاتصال عبر الانترنت، ويستعين المكتب لمكافحة هذه الجرائم بثلاث جهات هي:[2]

وحدة التحليل والتوثيق العلمي: وتختص بتحليل ومعالجة المعلومات الواردة من السلطات القضائية المختصة بمكافحة الجرائم المرتبطة بتكنولوجيا المعلومات والاتصالات، سواء على المستوى الوطني أو الدولي.

وحدة المساعدات التقنية: وهي مدعمة بتقنيات وبرامج متطورة من الناحية التقنية بهدف ضمان مساعدة فعالة في التحري والبحث وجمع الأدلة الإلكترونية، وتضم هذه الوحدة عددا من المحققين المتخصصين في الإجرام المعلوماتي.

وحدة العمليات: وتتشكل من أربع فرق، تختص الأولى بجرائم الاحتيال الواقعة على وسائل الدفع، أما البقية فتختص بالجرائم الواقعة على شبكات الاتصال.

ب- قسم الانترنت التابع للإدارة التقنية للبحوث القانونية والوثائقية: المعروف اختصارا ب: STRJD ينعقد له الاختصاص بجمع الأدلة الإلكترونية ومعالجتها وتحليلها، بحيث يستطيع رجال القانون من محققين وقضاة استخلاص دلالاتها.

بريطانيا: خصصت بريطانيا وحدة تجمع نخبة من رجال الشرطة المتخصصين في البحث والتنقيب عن الجرائم المرتبطة بالانترنت، كالجرائم الجنسية وخاصة الواقعة على الأحداث، وتضم هذه الوحدة ثمانين مفتشا، نصفهم متمركزون في لندن ضمن الوحدة الوطنية لمكافحة جرائم التقنية العالية، والنصف الباقي موزعون على الوحدات المحلية الأخرى، وتتلخص مهام هذه الوحدة في متابعة مرتكبي الجرائم الجنسية عبر الانترنت خصوصا تلك الواقعة على الأحداث، وكذلك قراصنة المعلومات، وجرائم نشر الفيروسات.[3]

---

[1] Béatrice Clément, op cit, p271.

[2] أيمن رمضان، المرجع السابق، ص429.

[3] صالح شنين، الحماية الجنائية للتجارة الإلكترونية، أطروحة دكتوراه في القانون الخاص، جامعة أبي بكر بلقايد، تلمسان 2013/2012، ص217.

مصر: استحدثت مصر بعض الآليات وهي:

– الإدارة العامة للتوثيق والمعلومات: تختص هذه الإدارة– ومقرها وزارة الداخلية– بمكافحة الجرائم المعلوماتية ومنها جرائم الاعتداء على التجارة الالكترونية، وهي في ذلك تختص بعمليات المتابعة الفنية لتلك الجرائم، ويبدأ عملها من خلال المتابعة الفنية والتحري عن الجرائم المبلغ عنها من الإدارات الأخرى، وذلك من خلال استخدام شبكة الانترنت وتحديد شخص المتهم، هذا من جهة، ومن جهة أخرى فهي تقوم بتحديد المتهم من خلال عملية التتبع، ويعتمد أسلوب عمل هذه الإدارة في معرفة شخص مرتكب الجريمة على استخدام البرامج الحديثة، وذلك عن طريق الاعتماد على بروتوكول IP الذي يتعامل من خلاله المتهم مع شبكة الانترنت.[1]

– الإدارة العامة لمكافحة جرائم الحاسب الآلي وشبكات المعلومات سنة 2005، وهي تابعة للإدارة العامة للمعلومات والتوثيق، وتختص بمكافحة الجرائم المعلوماتية، وتتألف من ضباط على درجة عالية من الحرفية والتخصص في تكنولوجيا الحاسب الآلي والانترنت، مقسمين إلى عدد من الأقسام وهي: قسم العمليات، قسم التأمين، قسم البحوث والمساعدات الفنية؛ فقسم العمليات يختص بالتصدي للجرائم التي تكون أجهزة الحاسب الآلي وسيلة لارتكابها في مجالات نظم المعلومات، وشبكات وقواعد البيانات، سواء من داخل الوزارة أو من خارجها، ويقوم أيضا بإخطار الأجهزة المختصة بأعمال المكافحة بالبيانات والمعلومات المتعلقة بالجريمة، والتنسيق معها لإجراء التحريات وعمليات الضبط في تلك الجرائم، كما يقوم بإعداد قاعدة بيانات عن جرائم المعلوماتية والأحكام الصادرة بشأنها، وهوية مرتكبيها، وإنشاء الملفات والسجلات والبطاقات اللازمة لهذه العملية، أما قسم التأمين فيختص بوضع الخطط والأساليب المستعملة في مجال تأمين نظم المعلومات والشبكات التابعة لأجهزة الوزارة، وتنفيذها بعد اعتمادها بالتنسيق مع الأجهزة المختصة، أما قسم البحوث والمساعدات الفنية فمهمته إعداد البحوث الفنية والقانونية في مجال تأمين نظم وشبكات المعلومات والحاسبات الآلية، ودراسة الظواهر الإجرامية المتعلقة بالمعلوماتية قصد الاستفادة منها بغية فهمها وتطوير أساليب مكافحتها، وهذا بالتنسيق مع الأجهزة المختصة، كما يقوم بدراسات حول مدى ملاءمة التشريعات

[1] أيمن رمضان، المرجع السابق، ص430.

العقابية للتصدي للجرائم الإلكترونية، بالإضافة إلى تقديم الدعم الفني وتوفير المساعدات الفنية وإبداء الرأي والمشورة للجهات المختصة في القضايا والوقائع المرتبطة بهذا النوع من الجرائم.[1]

الجزائر: أنشأت الجزائر على مستوى الدرك الوطني مركزا لمكافحة جرائم الانترنت، أوكلت إليه مهام البحث والتحقيق في مجال الجرائم الإلكترونية بصفة عامة، بالإضافة إلى هيئات أخرى، من مثل الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، التي تتولى حسب نص م14 من القانون 09-04 سالف الذكر تنشيط وتنسيق عمليات الوقاية من جرائم الاتصال والمعلومات ومكافحتها، ومساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشأن الجرائم ذات الصلة بتكنولوجيا الإعلام والاتصال، بما في ذلك تجميع المعلومات وإنجاز الخبرات القضائية، وتبادل المعلومات مع نظيرات الهيئة في خارج الوطن بهدف جمع كل المعطيات المفيدة في التعرف على مرتكبي الجرائم المعلوماتية وتحديد أمكنة تواجدهم.[2]

من الآليات التي تم إنشاؤها أيضا سلطات التصديق الإلكتروني: السلطة الوطنية للتصديق الإلكتروني، وهي سلطة إدارية مستقلة (م16 من القانون 15-03)، السلطة الحكومية للتصديق الإلكتروني (م26 من القانون 15-03)، والسلطة الاقتصادية للتصديق الإلكتروني (م29 من القانون 15-03).

---

[1] أيمن رمضان، المرجع السابق، ص431.

[2] صدر المرسوم الرئاسي رقم 15-261 المؤرخ في 08 أكتوبر 2015، ج ر 16 الصادرة في 08 أكتوبر 2015 ليحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، وقد تضمن ستة فصول وثلاث وأربعين مادة، ومن مهام هذه الهيئة مراقبة الاتصالات الإلكترونية وتجميع وتسجيل محتواها في حينها، والقيام بإجراءات التفتيش والحجز داخل منظومة معلوماتية (م21 من المرسوم سالف الذكر)، ويجوز للهيئة لتنفيذ عملية المراقبة أن تضع وحدة مراقبة واحدة أو أكثر مكونة من مستخدمين تقنيين تحت إدارة ومراقبة قاض بمساعدة ضابط أو أكثر من ضباط الشرطة القضائية المنتمين للهيئة (م22)، كما يجوز أن يقوم قضاة وضباط الشرطة القضائية التابعين للهيئة تفتيش أي مكان أو هيكل أو جهاز بلغ إلى علمهم أنه يحوز أو يستعمل وسائل وتجهيزات موجهة لمراقبة الاتصالات الإلكترونية (م30).

المطلب الثاني: التحقيق في الجرائم الواقعة على التجارة الإلكترونية.

يعالج هذا المطلب من خلال التطرق إلى خصائص ومميزات التحقيق في الجرائم الواقعة على التجارة الإلكترونية (الفرع الأول)، ثم إجراءات التحقيق في الجرائم الواقعة على التجارة الإلكترونية (الفرع الثاني).

الفرع الأول: خصائص التحقيق في الجرائم الواقعة على التجارة الإلكترونية.

نظرا للخصائص التي يتميز بها كل من المجرم المعلوماتي، والجرائم المعلوماتية أو الإلكترونية، فإن التحقيق في هذه الجرائم له بعض الخصوصية ليتلاءم وطبيعة الجرائم محل التحقيق.

أولا: مفهوم التحقيق في الجرائم الواقعة على التجارة الإلكترونية.

تبدأ عقب مرحلة الاستدلال أو الاستقصاء مرحلة ثانية من مراحل الدعوى العمومية، هي مرحلة التحقيق الابتدائي، التي تتسم بأهمية خاصة، لذا تخضعها التشريعات المقارنة لبعض المبادئ لضمان حقوق الدفاع من ناحية، وفعالية التحقيق ذاته من ناحية أخرى.[1]

عموما يمكننا القول أن هناك نوعين من أعمال التحقيق الابتدائي، النوع الأول يهدف إلى الكشف عن الحقيقة، ويطلق عليه إجراءات جمع الأدلة، كالانتقال للمعاينة، وندب الخبراء وسماع الشهود، وضبط الأشياء، والتفتيش، والاستجواب؛ أما النوع الثاني فهو أوامر التحقيق الهادفة إلى تأمين الأدلة ويطلق عليها إجراءات التحقيق الاحتياطية، من مثل أوامر الضبط والإحضار، والأمر بالحبس المؤقت وغيرها.[2]

يمارس مهام التحقيق القضائي في الجزائر قضاة يعينون لهذا الغرض،[3] فقد آثر المشرع الجزائري الفصل بين سلطتي التحقيق والادعاء على غرار نظيره في كل من فرنسا ولبنان، ودول أخرى عديدة، أما في دول أخرى كمصر فإن التحقيق تقوم به النيابة العامة كأصل عام، وقد قضت محكمة

---

[1] د. سليمان عبد المنعم، أصول الإجراءات الجزائية في التشريع والقضاء والفقه، المؤسسة الجامعية للدراسات والنشر والتوزيع، بيروت، لبنان 1997، ص511.

[2] المرجع نفسه، ص542.

[3] محمد حزيط، مذكرات في قانون الإجراءات الجزائية الجزائري، ط3، دار هومة، الجزائر 2008، ص81

النقض المصرية بأن: "النيابة العامة شعبة من شعب السلطة القضائية خول الشارع أعضاءها من بين ما خوله لهم سلطة التحقيق والادعاء العام طبقا لنظامها ولائحته".[1]

لاحتمال ارتباط الجرائم الواقعة على التجارة الإلكترونية بمختلف أنواع الجرائم الأخرى، فإن إجراءات التحقيق فيها تأخذ بجميع عناصر التحقيق الجنائي المتكامل، وتمر بالمراحل الفنية والشكلية نفسها، أما عناصر التحقيق الجزائي الأخرى، من معملية وفنية ونفسية وغيرها، فإن استخدامها يتوقف على ظروف كل جريمة، رغم ذلك فإن التحقيق في الجرائم المعلوماتية عامة له بعض الخصوصيات سواء من حيث الإجراءات الشكلية المتبعة، أو من حيث العناية بمسرح الجريمة وتكوين فرق العمل وأساليب تأمين الأدلة المادية وغير ذلك.[2]

ثانيا: صعوبة كشف الجرائم الواقعة على التجارة الإلكترونية.

تكمن صعوبة كشف الجرائم الواقعة في البيئة الإلكترونية نظرا للطبيعة الخاصة لهذه البيئة، والجرائم معا التي تتميز عن غيرها من الجرائم التقليدية، وتظهر هذه الصعوبة في:

1- سهولة إخفاء الجريمة.

الجرائم المعلوماتية بصفة عامة تكون مستترة خفية، لا يشعر المجني عليهم بها، ولا يلحظون وقوعها، حيث تتوافر لدى مرتكبي هذه الفئة من الجرائم مهارات فائقة، وذكاء وملكات لا يستهان بها، وخبرات معتبرة تمكنهم من إخفاء وحجب الأفعال المكونة للجريمة، حتى أن بعض الشركات لا تكتشف الاختلاسات إلا بعد إجراءات التدقيق التي تقوم بها على الحسابات،[3] وهذا ما جعل معتادي الجرائم الإلكترونية يطلقون على أنفسهم مصطلح النخبة، بحجة أنهم الأكثر معرفة بأسرار الحاسب الآلي ولغاتها المتميزة، وفي الوقت ذاته وبلهجة ساخرة فيها الكثير من التحدي والثقة الزائدة بالنفس، يطلقون على رجال إنفاذ القانون من شرطة ودرك... مصطلح الضعفاء أو القاصرين.[4]

---

[1] سامح أحمد بلتاجي موسى، الجوانب الإجرائية للحماية الجنائية لشبكة الانترنت، رسالة دكتوراه في الحقوق، جامعة الإسكندرية، مصر 2010، ص209.

[2] د. محمد الأمين البشري، التحقيق في جرائم الحاسب الآلي، بحث مقدم إلى بحوث مؤتمر القانون والكمبيوتر والانترنت من 1-3 مايو 2000، المجلد الثالث، ط3، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، 2004، ص1048.

[3] سامح أحمد، المرجع السابق، ص220.

[4] البشري، المرجع السابق، ص 1071.

والحقيقة التي لا يجب إنكارها أو غض الطرف عنها، أن المستوى التقني لرجال الأمن والمحققين العاملين في مجال مكافحة الجرائم المعلوماتية، خاصة بدول العالم الثالث، لا يبعث على الاطمئنان، وقد أثبت الواقع أن هنالك جرائم معلوماتية ارتكبت على مرأى ومسمع من رجال الأمن، بل قام بعض رجال الأمن بتقديم يد المساعدة لهؤلاء، عن جهل طبعا، أو على سبيل واجبات مهنتهم في مد العون للغير، بمعنى أنهم قد ساعدوا بعض مجرمي المعلوماتية على عملياتهم الإجرامية، وهم يحسبون أنهم يحسنون صنعا.[1]

هذا الأمر دفع الأجهزة الأمنية والقضائية في استيعاب المتخصصين في الحاسب الآلي والوسائل التقنية المتطورة الأخرى، ضمن إطاراتها،[2] كما جرى تدريب رجال الشرطة والقانون على تعلم واستخدام الوسائل التقنية الجديدة، إلا أن كل ذلك لن تكون له ثمرة واضحة في القريب العاجل على الأقل، وخاصة في دول العالم الثالث، لأسباب عديدة من بينها:[3]

– الميزانيات المالية المرصودة للإطار البشري في الأجهزة الحكومية غير كافية لاستقطاب النخبة المتميزة في مجال المعلوماتية، والتي تستقطبها عادة الشركات والقطاع الخاص.

– أجهزة الشرطة والنيابة وقضاة التحقيق، على عاتقهم مهام كثيرة، وأمامهم مجالات متنوعة عليهم القيام بها، وهم غير متفرغين للجرائم المعلوماتية وحدها، غير أن هذا لا يعني عدم تخصيص أقسام أو وحدات أو أقطاب تعنى بهذا النوع من الجرائم فقط.

– حداثة تجربة أجهزة إنفاذ القانون بالجرائم المعلوماتية عامة، وقلة الجرائم المكتشفة عمليا، لم تسمح لتلك الأجهزة من اكتساب الخبرة الكافية للعمل في هذا المجال.

انتشار الحاسب الآلي وغيره من الوسائل الإلكترونية الحديثة كالهاتف الجوال الذكي، على نطاق واسع وتنوع أنظمته وبرامجه، وسرعة المستجدات المتعلقة به، يجعل من العسير حصر أساليب الجريمة، وصورها وأنماطها، وبالتالي يتعذر تدريب المحققين على مواجهة بعض الحالات.

---

[1] المرجع نفسه، ص1050.

[2] وهذا ما فعله المشرع الجزائري، من خلال المادة 35 مكرر التي أضيفت بالأمر 15-02 المؤرخ في 23 يوليو 2015، المعدل والمتمم للأمر 66-155، ج ر40، الصادرة في 23 يوليو 2015، حيث أجازت هذه المادة للنيابة العامة الاستعانة في مسائل فنية بمساعدين متخصصين، يساهمون في مختلف مراحل الإجراءات تحت مسؤولية النيابة العامة، وينجزون تقارير تلخيصية أو تحليلية يجوز إرفاقها بالتماسات النيابة العامة.

[3] البشري، المرجع السابق، ص1072.

إزاء هذه المشاكل الفنية رأى البعض أن توكل مهمة التحقيق في الجرائم المعلوماتية إلى بيوت خبرة متخصصة في هذا المجال، خاصة وأن شركات عالمية قد تكونت وحققت نجاحات باهرة في كثير من الحالات؛ إلا أن هناك من يرى أن هذا الأمر ينطوي على مخاطر جمة، وفيه مساس بسيادة الدولة وهيبتها، بل قد يعرض أمنها القومي كله للخطر، فليس من الجائز وضع حقوق المجتمع تحت رحمة شركات همها تحقيق الكسب المالي، وهي غير مكلفة قانونا بتحقيق العدالة، كما أن هناك جرائم تتصل بأمن الدولة السياسي والاقتصادي ومصالحها العليا، ولا يجوز بحال من الأحوال أن يعهد التحقيق في هذه الجرائم لغير الأجهزة الحكومية المختصة.

2- الإحجام عن الإبلاغ في الجرائم المتعلقة بالتجارة الإلكترونية.

يعد عدم إبلاغ الأشخاص والجهات والمؤسسات المتضررة من الجرائم الإلكترونية معوقا بارزا من معوقات التحقيق.

والسؤال المطروح: لماذا يحجم الضحايا عن الإبلاغ؟

يكون الإحجام عن التبليغ لعدة أسباب، تختلف باختلاف الضحية نفسها، فالشركات التجارية مثلا تخشى على سمعتها في السوق، ولا ترغب أن تهتز ثقة عملائها فيها، لذلك تتكتم على ما تتعرض له من اعتداءات إلكترونية، رغم الخسائر المعتبرة التي تكون قد تكبدتها، بل حتى موظفوها قد لا يعلمون بما تعرضت له مؤسستهم من اعتداء، وتلجأ غالبا إلى إجراء تحقيقات ذاتية أو بمساعدة بيوت الخبرة، وتتخذ إجراءات إدارية داخلية.

وتظهر ظاهرة التكتم بقوة وعلى نحو أكثر حدة في المؤسسات المالية وخاصة البنوك، والمؤسسات الادخارية، ومؤسسات الإقراض والسمسرة، التي تخشى عادة من أن تؤدي الدعاية السلبية التي قد تنجم عن الإبلاغ عن هذه الجرائم وبدء التحقيق فيها، إلى تضاؤل الثقة في هذه المؤسسات، واستغلال المنافسين للأمر من أجل ضرب سمعتها مما ينجم عنه انصراف عملائها عنها، فيكون بذلك الضرر الذي يحيق بها نتيجة فقدان الثقة لدى المتعاملين معها، أكبر من المنفعة التي تجنيها من جراء متابعة المعتدين عليها، فتؤثر عدم الإبلاغ، مما حذا بالعض في الولايات المتحدة

الأمريكية إلى المطالبة بتضمين القوانين نصوصا توجب على موظفي هذه المؤسسات بالإبلاغ عن الجرائم تحت طائلة المسؤولية الجزائية.[1]

غير أنه عند عرض هذا الاقتراح على (لجنة خبراء مجلس أوربا) قوبل بالرفض، لسبب قانوني مؤداه أن المجني عليه أو الضحية التي ارتكبت في حقها الجريمة المعلوماتية، ستصبح متهمة أو جانية بعد أن كانت مجنيا عليها، كما أنه من غير المفيد معاقبة الشركة على ضرر هي من تتحمله أولا، ولذلك وردت اقتراحات أخرى بديلة منها الالتزام بإبلاغ جهة خاصة، أو إبلاغ سلطات إشرافية، وتشكيل أجهزة خاصة لتبادل المعلومات، وكذلك إصدار شهادة أمن خاصة تُمنح بعد عمل مراجعة وتدقيق من قبل هيئة خاصة من المراجعين، ويتعين على هذه الهيئة إبلاغ الشرطة بما تكتشفه من جرائم.[2]

كما أن الأفراد قد يحجمون عن الإبلاغ لأسباب كثيرة منها جهلهم التام بوقوع اعتداء عليهم، فقد لا ينتبهون للأمر إلا بعد مرور مدة زمنية معينة، مما يجعلهم يعتقدون أن لا طائل من وراء الإبلاغ، ناهيك عن تخوف البعض من القدح في سمعتهم ومهاراتهم، وتخوفهم من رميهم بالسذاجة وعدم الفطنة.

وعلى الصعيد الدولي، فإن من أسباب الإحجام عن الإبلاغ هو صعوبة الإبلاغ ذاته بالنسبة لهذا النوع من الجرائم، لعدم وجود جهات دولية تتولى تلقي البلاغات على مستوى دول العالم، وكذلك عدم وجود شبكة دولية لتبادل المعلومات الأمنية كما هو الحال بالنسبة لشبكة (يوروبول) التي تعمل في إطار الشرطة الدولية، وكما هو الحال بالنسبة لشبكة أنترانت التي تمثل اتحاد شركات عالمية تعمل بمعزل عما تواجهه شبكة الانترنت من مشكلات وثغرات.[3]

---

[1] سامح أحمد، المرجع السابق، ص221.

[2] د. عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والانترنت، دار الفكر الجامعي، الإسكندرية، مصر 2006، ص116.

[3] سامح أحمد، المرجع السابق، ص222. يراجع أيضا: د بيومي حجازي، المرجع السابق، ص117.

ثالثا: سير التحقيق في الجرائم الواقعة على التجارة الإلكترونية.

يتوجب على الأجهزة الأمنية والقضائية أن تعمل على توفير الإمكانات التقنية اللازمة، للتحقيق في الجرائم المعلوماتية عامة، وعليها بذل الجهد لاستقطاب الكفاءات المهنية المتخصصة في هذا المجال، وضرورة الاستعانة بالمتخصصين الذين لهم علاقة من قريب أو بعيد بالموضوع، في جميع مراحل الدعوى العمومية، منذ كشف الجريمة وإلى غاية النطق بالحكم النهائي فيها. ومن أجل ذلك اقترح البعض أسلوبا خاصا لسير التحقيق في هذه الجرائم، بحيث يعتمد على الخبرة الفنية والكفاءة المهنية، ويكون ذلك من خلال توفير وتحقيق العناصر التالية:

– أن يستعين المحقق في عمله بالخبير، ويقومان بتبادل المعلومات قبل بدء التحقيق، وأخذ أقوال الشهود والمشتبه فيهم، واستجواب المتهمين، بحيث يتفقان على طريقة ترتيب المتهمين والشهود، وطريقة توجيه الأسئلة إليهم، ويقوم الخبير بشرح الأبعاد والمعطيات الفنية، والنقاط التي يُرغب في الحصول عليها من المحقق معهم.

– يوضح خبير المعلوماتية للمحقق كافة الأمور التقنية اللازمة للتحقيق، وكافة المصطلحات الفنية التي يمكن أن تستخدم، مع بيان معانيها، لتتم الاستفادة منها عند الحاجة إليها.

– يقوم المحقق بمساعدة الخبير بعملية حصر لكافة النقاط المطلوب إيضاحها من قبل كل منهما، ليتولى المحقق ترتيب هذه النقاط قبل البدء في التحقيق.

– يقوم المحقق بوضع خطة سير محكمة للتحقيق على ضوء ما لديه من معطيات أخرى حول القضية، وما يتراءى له من اعتبارات مصلحة التحقيق.

– من الأفضل أن يتم أخذ أقوال الشهود واستجواب المتهمين من قبل المحقق، بحضور الخبير المعلوماتي، الذي يتاح له توجيه بعض الأسئلة الفرعية التقنية أثناء الاستجواب، وفق الكيفية التي يتم الاتفاق عليها مسبقا، مع مراعاة عدم تدخل الخبير في اختصاص المحقق.

– ضرورة التنسيق بين المحقق والخبير في الحصول على البيانات المخزنة في الحاسب الآلي وملحقاته، الخاص بالمتهم أو الشاهد الذي يجري التحقيق معه؛ فغالبا ما يحتفظ مجرمو المعلوماتية بخططهم ومعلوماتهم على أقراص أو في ذاكرة الحاسب الآلي أو على شرائح معينة، مع مراعاة عدم إجبار

الشاهد أو المتهم الذي يُجرى التحقيق معه على تقديم دليل يدينه طبقا لما هو معمول به في القواعد العامة.[1]

وينبغي مراعاة بعض الأمور أثناء سير التحقيق في الجرائم المعلوماتية عامة من بينها:

– تفادي ضياع الوقت في التحقيق حول بعض الجرائم المعلوماتية التي لا يمكن اكتشافها لأن الأدلة اللازمة لذلك قد تم القضاء عليها.

– ضرورة تعاون المحققين والخبراء مع الإطارات المختصة في مجال المعلوماتية للمؤسسة المجني عليها، للحصول على أكبر قدر من المعلومات الفنية اللازمة للتحقيق.

– الاعتناء بإصدار الأوامر القضائية في أسرع وقت ممكن لتفتيش وضبط أجهزة الحاسب الآلي وملحقاتها، وبرمجياتها اللازمة لكشف البيانات المخزنة، ووضع كل التدابير اللازمة للمحافظة عليها وحسن استخدامها.

– مراعاة حفظ الأدلة بالطرق الملائمة لكل حالة على حدة، حتى يتم تقديمها للمحكمة، وهي على حالتها التي ضبطت عليها.

– الاستعانة بالتقنيات المتطورة في مواجهة الجرائم المعلوماتية.

– مراعاة عدم مخالفة الإجراءات والقوانين السارية، خاصة ما تعلق منها بالحقوق الشخصية للأفراد، ومنها سرية البريد الإلكتروني.[2]

– ينبغي التنقل السريع لمعاينة مسرح الجريمة الإلكترونية، حتى لا يقدم بعض الأشخاص على إلغاء أو تحريف رسائل البريد الإلكتروني الموجودة على جهاز المتهم والمتعلقة بموضوع الجريمة، أو تغيير الرقم السري الخاص بالحاسب الآلي، أو مسح برامج خاص بالاختراق يكون قد استخدم في ارتكاب الجريمة؛ وتنص القواعد العامة على ضرورة عدم التباطؤ في جمع الأدلة وعدم التردد في مباشرة الإجراءات المناسبة حتى لا تضيع الفائدة من اتخاذها في وقتها المناسب.[3]

– ينبغي تحري الدقة في فحص وحصر الأدلة التي خلفها المجرم المعلوماتي، من ذلك عدم إغفال ملاحظة ما حتى ولو بدت غير ذات قيمة.

---

[1] سامح أحمد، المرجع السابق، ص226.

[2] المرجع نفسه، ص226.

[3] د. خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، دار الفكر الجامعي، الإسكندرية، مصر 2010، ص129.

– ينبغي عدم الاكتفاء باعتراف المتهم دون إثبات باقي أدلة الجريمة الإلكترونية، إذ أن مجموع هذه الأدلة لازم لتأكيد صحة الاعتراف، أو لإظهار كذبه، بالإضافة إلى احتمال العدول عن الاعتراف أمام المحكمة.[1]

– ينبغي على المحقق عدم ترك ثغرات في التحقيق، كما ينبغي عليه تكييف الجريمة المعلوماتية، تكييفا قانونيا صحيحا.[2]

الفرع الثاني: إجراءات التحقيق في الجرائم الواقعة على التجارة الإلكترونية.

تهدف إجراءات التحقيق في الجرائم الواقعة على التجارة الإلكترونية إلى جمع الأدلة الإلكترونية أو الرقمية كما يسميها بعض الفقه، وفحصها ونسبتها إلى فاعلها؛ ولم ترد إجراءات التحقيق في القانون على سبيل الحصر، حيث يجوز مباشرة أي إجراء يفيد في كشف الحقيقة شريطة أن يكون هذا الإجراء مشروعا.[3]

غير أن الخصوصية التي تتميز بها الجرائم الإلكترونية جعلت المشرع يضفي إجراءات حديثة لجمع الأدلة الإلكترونية بالإضافة إلى الإجراءات التقليدية.

أولا: الإجراءات التقليدية في تحقيق الجرائم الإلكترونية.

نظم المشرع في قوانين الإجراءات الجزائية المقارنة طرق جمع الأدلة من خلال إجراءات تحقيق هدفُها الوصول إلى استنباط الدليل، وأهم هذه الإجراءات، المعاينة، التفتيش، الاستجواب والمواجهة، والشهادة، وضبط الأدلة، وندب الخبراء.

نتناول هذه الطرق التي حددها القانون، ونحاول أن نلمس مدى قدرتها على المساعدة في الحصول على الأدلة في الجرائم الإلكترونية.

---

[1] خالد ممدوح إبراهيم، المرجع السابق، ص130.

[2] المرجع نفسه، ص131.

[3] المرجع نفسه، ص144.

1-الانتقال والمعاينة في الجريمة الإلكترونية.

يعني الانتقال ذهاب المحقق إلى مكان ارتكاب الجريمة، حيث توجد آثارها وأدلتها، أما المعاينة فهي رؤية وإثبات حالة مكان ارتكاب الجريمة، وجمع الآثار المتعلقة بها، وتحديد كيفية حدوثها، بمعنى مشاهدة وإثبات الآثار المادية التي خلفها ارتكاب الجريمة،[1] وقد تطرق المشرع الجزائري إلى المعاينة في م79 ق إ ج ، م80 ق إ ج.

وللمعاينة دور هام، فكلما سارع المحقق في الانتقال إلى مسرح الجريمة، ساعد ذلك على الوصول إلى الحقيقة قبل أن تمتد يد العبث إلى الأدلة، وأمكن اتخاذ إجراءات فورية كسماع الشهود الحاضرين مرة واحدة ومواجهتهم بعضهم ببعض، أو القبض على المتهم الحاضر.[2]

وقد قضي أن المعاينة من إجراءات التحقيق التي يترك أمر تقدير لزوم القيام بها إلى السلطة التي تباشر التحقيق، وقضي أيضا بأن المكان الذي يختاره المحقق لإجراء التحقيق متروك لتقديره وحسن اختياره حرصا على صالح التحقيق وسرعة إجرائه.[3]

المعاينة واردة في كل الجرائم، إلا أن أهميتها العملية تتضاءل بالنسبة لبعضها ومن ذلك الجرائم الإلكترونية، إذ أن الجريمة التقليدية غالبا ما يكون لها مسرح تجري عليه الأحداث، وتخلف آثارا مادية تحصّل منها الأدلة، أما مسرح الجريمة الإلكترونية فيتضاءل دوره في الإفصاح عن الوقائع المؤدية إلى الأدلة، ذلك أن الجريمة الإلكترونية قلما تخلف آثارا مادية، كما أن الكثير من الأشخاص قد يترددون على مسرح الجريمة خلال الفترة الفاصلة بين ارتكاب الجريمة ولحظة اكتشافها أو بدء التحقيق فيها، مما قد ينتج عنه إتلاف أو تغيير للأدلة المادية للجريمة إن وجدت،[4] ناهيك عن إمكانية التلاعب في البيانات عن بعد، أو محوها عن طريق التدخل من قبل وحدة طرفية من قبل المجرم المعلوماتي.[5]

---

[1] أسامة عبد الله قايد، المرجع السابق، ص 433.

[2] المرجع نفسه، ص434.

[3] بيومي حجازي، المرجع السابق، ص310.

[4] د عبد الفتاح بيومي حجازي، الإثبات الجنائي في جرائم الكمبيوتر والانترنت، دار الكتب القانونية، المحلة الكبرى، القاهرة 2007، ص144.

[5] خالد ممدوح إبراهيم، المرجع السابق، ص154.

ولذلك حرصت معظم التشريعات تحت طائلة العقاب على أي شخص أن يقوم بأي تغيير على مسرح الجريمة، من ذلك م43 من ق إ ج، وم1/55 ق إ ج ف، وهذه النصوص عامة تطبق على الجرائم التقليدية وكذا جرائم المعلوماتية ويترتب عن ذلك ضرورة المحافظة على مكونات الحاسب الآلي المادية كالأشرطة والأقراص والطابعة، والشرائح وغيرها، أما المكونات غير المادية فتتطلب إجراءات خاصة،[1] حسب نوع الجريمة المرتكبة، والملاحظ أن الآثار المعلوماتية أو الرقمية من الممكن أن تكون ثرية للغاية، بما تحويه من معلومات، وهذه إحدى صعوبات التحقيق في الجرائم المعلوماتية، فصفحات المواقع، والبريد الإلكتروني، والفيديو الرقمي، الصوت الرقمي، غرف الدردشة والمحادثة، الملفات المخزنة في الحاسب الشخصي، الصورة المرئية، الدخول للخدمة والاتصال بالانترنت عن طريق مزود الخدمات، كل هذه الوسائل والأدوات والوسائط تحوي دون شك في كثير من الأحيان أدلة كثيرة تفيد في كشف الحقيقة بشأن الجريمة محل التحقيق.[2]

في إطار الجرائم المعلوماتية، فإن عملية الانتقال والمعاينة تتم بصورة مغايرة لما يحدث بالنسبة للجرائم التقليدية، إذ قد يكون الانتقال للمعاينة افتراضيا فقط، ويجوز للمحقق القيام بذلك من مكتبه أو من أحد مقاهي الانترنت، أو اللجوء إلى مقر مزود الانترنت الذي يعد أفضل مكان يمكن من خلاله إجراء المعاينة.[3]

ويرى البعض ضرورة مراعاة الآتي قبل التحرك إلى مسرح الجريمة:

– وجود معلومات مسبقة عن مكان الجريمة من حيث عدد الأجهزة المطلوب معاينتها وشبكاتها.

– وجود خريطة توضح الموقع الذي ستتم معاينته، وتفاصيل المبنى أو الطابق موضوع البلاغ، وعدد الأجهزة والخزائن والملفات.

– تحديد الأجهزة المحتمل تورطها في الجريمة الإلكترونية، لكي يتم تحديد كيفية التعامل معها فنيا قبل المعاينة.

– تأمين الأجهزة والمعدات التي يستعان بها في عملية المعاينة، سواء كانت أجهزة أو برامج صعبة أو لينة.

---

[1] عائشة بن قارة، المرجع السابق، ص83.

[2] سامح أحمد، المرجع السابق، ص234.

[3] المرجع نفسه، ص235.

– إعداد الفريق المتخصص الذي يتولى المعاينة من الخبراء ورجال الضبط والأمن.

– تحديد البيانات والمهام والاختصاصات المطلوبة من كل عضو في فريق المعاينة، حتى تتكامل الاختصاصات ولا تتداخل.

– إعداد خطة المعاينة موضحة بالرسومات مع تمام المراجعة التي تكلف تنفيذها على الوجه الأكمل.

– تأمين عدم انقطاع التيار الكهربائي، لأن انقطاعه قد يسبب محو المعلومات من الذاكرة، من جراء التوقف غير العادي لجهاز الحاسب الآلي، وبالتالي فقدان كافة العمليات التي كان يتم تشغيلها، واتصالات الشبكة وأنظمة الملفات الثابتة.[1]

– مراعاة أن تتم كل هذه الإجراءات وفق مبدأ المشروعية، وفي إطار ما تنص عليه القوانين.[2]

ومن الإجراءات التي يتعين اتباعها عند إجراء المعاينة في البيئة الرقمية ما يلي:[3]

– القيام بتصوير جهاز الحاسب الآلي الذي ارتكبت عن طريقه الجريمة، وما قد يتصل به من أجهزة طرفية، ومحتوياته وأوضاع المكان الذي يوجد به، مع العناية بتصوير أجزائه الخلفية وبقية ملحقاته.

– وضع حراسة كافية على مكان المعاينة، ومراقبة التحركات داخل مسرح الجريمة.

– ملاحظة الطريقة التي أعد بها النظام المعلوماتي، والآثار التي يخلفها، والسجلات الإلكترونية التي تزود شبكات المعلومات بغية معرفة موقع الاتصال، ونوع الجهاز المتصل، عن طريق الدخول إلى النظام أو الموقع.

– ملاحظة حالة التوصيلات والكابلات المتصلة بكل مكونات النظام، بقصد تحليل كل البيانات ومقارنتها.

– عدم التسرع في نقل المواد المعلوماتية خارج مسرح الجريمة، إلا بعد التأكد تماما من خلو المحيط الخارجي للحاسب الآلي من مجالات القوة المغناطيسية التي قد تسبب إتلافا للبيانات المخزنة.

---

[1] عائشة بن قارة، المرجع السابق، ص86.

[2] بيومي حجازي، المرجع السابق، ص145. وكذلك للمؤلف نفسه، مبادئ الإجراءات الجنائية... المرجع السابق، ص316. ويراجع أيضا: البشري، المرجع السابق، ص1054.

[3] بيومي حجازي، مبادئ الإجراءات...المرجع السابق، ص317، وكذلك للمؤلف نفسه، جرائم الكمبيوتر...المرجع السابق، ص146. وعائشة بن قارة، المرجع السابق، ص86-87. وخالد ممدوح إبراهيم، المرجع السابق، ص172 وما بعدها.

– التحفظ على محتويات سلة المهملات، وما فيها من أوراق ممزقة وشرائط وأقراص ممغنطة غير سليمة أو محطمة، والتحفظ على مستندات الإدخال والمخرجات الورقية لأنه من المحتمل أن تكون لها صلة بالجريمة.

– القيام بالمعاينة من قبل فئة معينة من الباحثين والمحققين الذين تتوفر لديهم الكفاءة العلمية، والخبرة الفنية في مجال الجرائم المعلوماتية، والذين يكونون قد تلقوا تدريبا كافيا على التعامل مع نوعية الآثار والأدلة التي يحويها مسرح الجريمة الإلكتروني؛ ففي فرنسا مثلا يقوم فريق مكون من ثلاثة عشر شرطيا بالإشراف على تنفيذ المهمات التي يعهد بها إليه، وكلهم قد تلقوا تدريبات كافية ومتخصصة، إلى جانب تخصصهم الأصلي في مجال تكنولوجيا المعلومات، وهم يقومون بمرافقة المحققين أثناء المعاينة والتفتيش، حيث يفحصون كل جهاز، وينقلون نسخة من الأسطوانة الصلبة، وبيانات البريد الإلكتروني، ثم يقومون بعمل تقرير يرسل إلى قاضي التحقيق، وهم يستعينون ببرامج تمكنهم من قراءة الحاسبات الآلية المحمولة.[1]

2- التفتيش في الجرائم الإلكترونية.

التفتيش عمل من أعمال التحقيق، يستهدف كشف الحقيقة بشأن الجرم الواقع، ومدى ثبوته في مواجهة المتهم. ولقاضي التحقيق اللجوء إلى التفتيش إما بنفسه، وإما أن يأذن بذلك لأحد ضباط الشرطة القضائية من خلال الإنابة القضائية، ويشمل التفتيش الأشخاص والمنازل، وهو من الإجراءات الخطيرة التي تمس بحريات الأشخاص وحرمة منازلهم، لذا أحاطته الدساتير والمواثيق الدولية، والتشريعات المقارنة بعدد من القيود كضمانات لحريات الأفراد ولمبدأ المشروعية.[2]

والتفتيش ليس غاية في حد ذاته، وإنما هو وسيلة لغاية هي الوصول إلى أدلة مادية تسهم في ظهور الحقيقة، ولذلك فإن التفتيش في البيئة الإلكترونية أو الرقمية يعد من أخطر المراحل وأدقها، ولقد ثار جدل فقهي حول مدى صلاحية مكونات الحاسب الآلي المعنوية للتفتيش؟ وما هي الضوابط التي يجب مراعاتها أثناء عمليات التفتيش في البيئة الرقمية؟

[1] سامح أحمد، المرجع السابق، ص237.

[2] د. سليمان عبد المنعم، المرجع السابق، ص551.

أ- مدى خضوع مكونات الحاسب الآلي للتفتيش.

إن المكونات المادية للحاسب الآلي ولواحقه لا تثير أية مشكلة بخصوص جواز انطباق قواعد التفتيش التقليدية عليها، بالشروط ذاتها المطبقة بخصوص التفتيش في الجرائم التقليدية، بمعنى أن حكم تلك المكونات يتوقف على طبيعة الأماكن الموجودة فيها، سواء الأماكن العامة أو الخاصة، فإذا كانت موجودة في مكان خاص كمنزل المتهم أو مكتبه فلا يجوز تفتيشها إلا في الحالات التي يجوز فيها تفتيش المسكن، وبالضمانات المقررة قانونا، وفي الأوقات المقررة للتفتيش، وهذا ما أخذت به بعض التشريعات ومنها التشريع المصري،[1]إلا أن المشرع الجزائري قد خالف نص م64 من ق إ ج وأورد عليها استثناءات بموجب القانون رقم 22/06 المعدل للأمر 66-155 المتضمن قانون الإجراءات الجزائية، إذ استثنى تطبيق هذه الضمانات على بعض الجرائم لخطورتها، ومن بينها **الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات**، وأجاز المشرع بذلك إجراء التفتيش في كل محل سكني أو غير سكني في كل ساعة من ساعات النهار أو الليل، شريطة الحصول على إذن مسبق من وكيل الجمهورية المختص (م47 ق إ ج).

ربما كان من الأفضل أن ينص المشرع على أن يكون الحصول على الإذن المسبق من قاضي التحقيق، ما دام أن المشرع الجزائري قد أخذ بنظام الفصل بين الادعاء والتحقيق.

أما المكونات المنطقية أو المعنوية للحاسب الآلي فقد ثار خلاف تشريعي وفقهي بشأنها، بين مجيز لتفتيشها نظرا لعموم النص الوارد "ضبط أي شيء" ليشمل مكونات الحاسب الآلي المادية والمعنوية، وبين رافض لذلك باعتبار أن مفهوم التفتيش مفهوم مادي، وهو لا ينطبق على مكونات الحاسب الآلي المعنوية، وكان هذا الرأي سائدا عند بعض الفقه الفرنسي إلى أن قام المشرع بتعديل نصوص التفتيش بموجب القانون رقم 245-2004 المؤرخ في 2004/06/21، وقام بإضافة عبارة "المعطيات المعلوماتية" في م94 ق إ ج ف.[2]

وكانت الاتفاقية الأوربية حول الجرائم المعلوماتية، قد نصت في م19 من القسم الرابع على أن لكل دولة طرف أن تسن من القوانين ما هو ضروري لتمكين السلطات المختصة بالتفتيش

[1] عائشة بن قارة، المرجع السابق، ص89. ويراجع أيضا: نعيم سعيداني، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة ماجستير في العلوم القانونية، تخصص علوم جنائية، جامعة الحاج لخضر، باتنة 2013/2012.ص145

[2] عائشة بن قارة، المرجع السابق، ص91.

أو الدخول إلى نظام الكمبيوتر أو جزء منه أو المعلومات المخزنة به، وكذا إلى الوسائط التي يتم تخزين معلومات الكمبيوتر بها ما دامت مخزنة في إقليمها.

تطرق المشرع الجزائري إلى تفتيش المنظومات المعلوماتية في م5 من القانون 09-04،[1] والتي نصت: "يجوز للسلطات القضائية المختصة، وكذا ضبط الشرطة القضائية...الدخول بغرض التفتيش ولو عن بعد إلى: أ) منظومة معلوماتية أو جزء منها وكذا المعطيات المعلوماتية المخزنة فيها، ب) منظومة تخزين معلوماتية، في الحالة المنصوص عليها في الفقرة أ، إذا كانت هنالك أسباب تدعو للاعتقاد بأن المعطيات المبحوث عنها مخزنة في منظومة معلوماتية أخرى وأن هذه المعطيات يمكن الدخول إليها انطلاقا من المنظومة الأولى، يجوز تمديد التفتيش بسرعة إلى هذه المنظومة أو جزء منها، بعد إعلام السلطة القضائية المختصة مسبقا بذلك...."

كما أن الاتفاقية العربية لمكافحة جرائم تقنية المعلومات المحررة بالقاهرة بتاريخ 2010/12/21، والتي صادقت عليها الجزائر نصت في م1/26 منها بأن تلتزم كل دولة طرف بتبني الإجراءات الضرورية لتمكين سلطاتها المختصة من التفتيش أو الوصول إلى تقنية معلومات أو جزء منها، والمعلومات المخزنة فيها أو المخزنة عليها، وكذا الوصول إلى بيئة أو وسيط تخزين معلومات تقنية معلومات والذي قد تكون معلومات التقنية مخزنة فيه أو عليه.

ومن الآراء الفقهية الأخرى حول المكونات المنطقية أو المعنوية للحاسب الآلي نجد فريقا فقهيا يذهب إلى القول بضرورة النظر إلى الواقع العملي، الذي يقتضي أن يقع الضبط على بيانات الحاسب إذا اتخذت شكلا ماديا، ومعنى ذلك أن البيانات المنفردة عن الدعامات لا تعد من قبيل الأشياء، وبالتالي لا يمكن ضبطها، بيد أنه إذا تم طبع هذه البيانات، فإن مطبوعاتها تعد من الأشياء الملموسة المحسوسة التي يجوز ضبطها.[2]

هناك اتجاه فقهي آخر يرى أن الأساس في تحديد مدلول الشيء فيما يخص مكونات الحاسب الآلي هو تحديد مدلول مصطلح المادة في العلوم الطبيعية، وكذا معرفة خصائص وكنه

[1] المؤرخ في 14 شعبان 1430هـ الموافق 5 غشت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، ج ر عدد 47 الصادر في 16 غشت 2009.

[2] سامح أحمد، المرجع السابق، ص253.

مكونات الحاسب المعنوية أو المنطقية؛ وبناء عليه يرى هذا الاتجاه أن البيانات والمكونات المنطقية للحاسب الآلي ليست من قبيل الشيء المعنوي كالآراء والأفكار والحقوق، بل يجوز اعتبارها أشياء لها وجود في العالم الخارجي الملموس، وهي شبيهة بالتيار الكهربائي، لذا يجوز أن يرد عليها الضبط والتفتيش، وهذا ما ذهبت إليه محكمة باريس الابتدائية في حكم لها، حينما قضت بأنه لا يوجد اختلاف في الطبيعة بين مخرجات البرامج وبين البرامج المستغلة، وكذلك وصفت محكمة جنح بروكسل هذه البيانات أو المكونات المنطقية بأنها تعد من قبيل الأشياء المحسوسة التي لها وجود مادي حقيقي.[1]

بنص المشرع الجزائري الصريح على تفتيش المنظومة المعلوماتية في م05 من القانون 09-04 يكون قد قطع الخلاف الفقهي حول جواز تفتيش المكونات المعنوية للحاسب الآلي من عدمه، كما أنه أجاز في الفقرة الأخيرة من المادة نفسها أن تستعين السلطات المكلفة بالتفتيش كل شخص له دراية بعمل المنظومة المعلوماتية محل البحث أو بالتدابير المتخذة لحماية المعطيات المعلوماتية التي تتضمنها، قصد مساعدتها وتزويدها بكل المعلومات الضرورية لإنجاز مهمتها.

ب- مدى قابلية شبكات الحاسب الآلي للتفتيش (التفتيش عن بعد).

ترتبط أجهزة الحاسب الآلي أحيانا ببعضها بعضا عن طريق شبكات، قد تكون داخل الشركة أو المؤسسة أو فروعها داخل الحدود السياسية لدولة واحدة، أو خارجها كأن يرتبط جهاز في فرع لشركة أم ببلد معين مع أجهزة أخرى في فروع تابعة لهذه الشركة في بلدان أخرى.

هذا الأمر يعقد من التحديات التي تقف أمام التفتيش والضبط. والسؤال المطروح: هل يمتد تفتيش حاسب معين إلى الأجهزة المرتبطة به سواء كانت موجودة داخل البلاد أم خارجها؟

الحالة الأولى: أن يكون الحاسب المراد تفتيشه موجودا في مكان آخر داخل الدولة.

بمعنى أن يتصل حاسب المتهم بحاسب آخر أو نهاية طرفية موجودة في مكان آخر داخل الدولة نفسها.

من المعلوم أن إذن التفتيش في الجرائم التقليدية يجب أن يحدد مكان ومحل التفتيش، ومكان التفتيش في الجرائم الإلكترونية هو المقر الذي به الجهاز المراد تفتيشه.

[1] سامح أحمد، المرجع السابق، ص254-255.

أجازت التشريعات المقارنة امتداد التفتيش إلى سجلات البيانات التي تكون في موقع آخر من الدولة، منها القانون الألماني، والقانون البلجيكي، والقانون الأسترالي.[1] وأجاز المشرع الأمريكي أن يمتد التفتيش الصادر بتفتيش مقر شركة معينة إلى فروع تلك الشركة الكائنة في العقار نفسه.[2] كما أجازه المشرع الجزائري في م05 من القانون 09-04 "... ولو عن بعد".

أما م1/17 من القانون الفرنسي رقم 239 لسنة 2003 بشأن الأمن الداخلي الصادر في 2003/03/18، فقد أجازت لرجال الضبط القضائي من درجة ضباط وغيرهم من رجال الضبط القضائي تحت مسؤولية الضباط، أن يدخلوا عن طريق الأنظمة المعلوماتية المثبتة في الأماكن التي يتم فيها التفتيش على البيانات التي تهم التحقيق والمخزنة في النظام المذكور أو في أي نظام معلوماتي آخر، ما دامت هذه البيانات متصلة في شبكة واحدة مع النظام الرئيس، أو يتم الدخول إليها أو تكون متاحة ابتداء من النظام الرئيس.[3]

وكانت اتفاقية بودابست لعام 2001 قد نصت في م19 من القسم الرابع على: "من حق السلطة القائمة بتفتيش الكمبيوتر المتواجد في دائرة اختصاصاتها أن تقوم في حالة الاستعجال بمد نطاق التفتيش إلى أي جهاز آخر، إذا كانت المعلومات المخزنة يتم الدخول إليها من الكمبيوتر الأصلي محل التفتيش".

أما الاتفاقية العربية لمكافحة جرائم تقنية المعلومات سالفة الذكر فقد نصت في م2/26 على أن "تلتزم كل دولة طرف بتبني الإجراءات الضرورية لتمكين السلطات المختصة من التفتيش أو الوصول إلى تقنية معلومات معينة أو جزء منها...فيجوز توسيع نطاق التفتيش والوصول للتقنية الأخرى".

وبخصوص تفتيش الحاسبات الآلية التي تقع في أماكن عامة كالحاسبات الشخصية التي يحملها الشخص خارج منزله، أو الهواتف الذكية، فإن تفتيش أنظمتها لا يكون جائزا إلا في الأحوال التي يجيز فيها القانون تفتيش شخصه، باعتبار أن تفتيش الشخص يشمل ذاته وكل ما في حوزته

[1] د. حسين بن سعيد الغافري، السياسة الجنائية في مواجهة جرائم الانترنت، دراسة مقارنة، دار النهضة العربية، القاهرة 2009، ص482.

[2] سامح أحمد، المرجع السابق، ص256.

[3] عائشة بن قارة، المرجع السابق، ص94.

وقت هذا التفتيش، سواء أكان ملكا له أم لغيره، وفي الحالة التي يكون فيها الجهاز المراد تفتيشه داخل منزل أحد الأشخاص، فإنه تسري عليه القيود التي ينص عليها القانون بالنسبة لتفتيش مسكن المتهم أو تفتيش منزل غير المتهم.[1]

يرى البعض ضرورة استصدار قوانين خاصة تغطي هذه الحالة (حالة وجود الجهاز بمكان آخر في الدولة)، وعدم الاكتفاء بالقواعد العامة الموجودة حاليا لأنها قاصرة عن تحقيق المطلوب خاصة في الحالتين الآتيتين:[2]

– إذا كان الجهاز المتصل بالجهاز الذي صدر الإذن بتفتيشه ينتمي إلى شخص غير المتهم، ومن ثم يتعين تفتيش الأجهزة المرتبطة به بناء على الإذن الأول، وهذا يتناقض مع بعض التشريعات الإجرائية ومنها التشريع المصري الذي تتولى النيابة فيه أمور التحقيق، والذي نص في م206 ق إ ج م، على أنه يشترط لاتخاذ أي إجراء من إجراءات تفتيش غير المتهم أو منزل غير المتهم الحصول مسبقا على أمر مسبب من القاضي الجزئي بعد اطلاعه على الأوراق.كما تثور شكوك في هذه الحالة إذا تم هذا التفتيش دون إخطار غير المتهم أو من ينوب عنه.

– في حالة التلبس لا يُشترط الحصول مسبقا على إذن لتفتيش الجهاز، وفي هذه الحالة قد تقوم الضبطية بتفتيش أجهزة غير المتهم المرتبطة بجهازه، باستخدام برامج معينة، فما مدى مشروعية هذا الفعل؟ خاصة وأنه يتم دون الحصول على إذن مسبق.[3]

الحالة الثانية: أن يكون الحاسب أو الجهاز المراد تفتيشه متصلا بنهاية طرفية أو جهاز آخر خارج حدود الدولة.

من المشاكل التي تواجه القائمين على جمع الدليل الإلكتروني، قيام مرتكبي الجرائم بتخزين بياناتهم في أنظمة تقنية خارج الدولة، مستخدمين في ذلك شبكة الاتصالات البعدية، بهدف عرقلة سير التحقيق ومن ثم الإفلات من العقاب، نتيجة تمسك كل دولة بسيادتها،[4] لذا ينبغي أن يتم التفتيش الإلكتروني في إطار اتفاقيات ثنائية تبرم بين الدول المعنية، وهذا يدخل ضمن إطار التعاون

[1] الغافري، المرجع السابق، ص485-486.

[2] عائشة بن قارة، المرجع السابق، ص96.

[3] المرجع نفسه، ص96.

[4] الغافري، المرجع السابق، ص484.

الدولي في مجال مكافحة ومجابهة الجرائم الإلكترونية، وهذا ما تطرقت له م05 من القانون 09-04 في إحدى فقراتها:"إذا تبين مسبقا بأن المعطيات المبحوث عنها والتي يمكن الدخول إليها انطلاقا من المنظومة الأولى مخزنة في منظمة معلوماتية تقع خارج الإقليم الوطني، فإن الحصول عليها يكون بمساعدة السلطات الأجنبية المختصة طبقا للاتفاقيات الدولية ذات الصلة، ووفقا لمبدأ المعاملة بالمثل".

وقد أكد المجلس الأوربي في التوجيه رقم 17 لسنة 1995 على جواز امتداد نطاق تفتيش الحاسب إلى النظام المتواجد في الخارج، إذا كانت هناك ضرورة لاتخاذ إجراءات عاجلة في هذا الصدد، ويتوجب حينها الحصول على موافقة الدولة التي يمتد التفتيش إلى الأجهزة أو النظام المتواجد في إقليمها، كي يكون هذا التفتيش ذا أساس قانوني، ولا يمثل انتهاكا لسيادة تلك الدولة.[1]

وكتطبيق لهذا الإجراء الأخير فقد حدث في ألمانيا أثناء القيام بإجراءات التحقيق عن جريمة غش وقعت في بيانات حاسب آلي، التماس مساعدة سويسرا، حيث بينت التحقيقات وجود اتصال بين الحاسب الآلي الموجود في ألمانيا وبين شبكة اتصالات في سويسرا يتم تخزين بيانات المشروعات فيها.[2]

غير أن م32 من الاتفاقية الأوربية بشأن الجرائم المعلوماتية سالفة الذكر، أجازت الولوج بغرض التفتيش والضبط في أجهزة أو شبكات تابعة لدولة أخرى دون أخذ الإذن منها في حالتين: إذا تعلق التفتيش بمعلومات أو بيانات مباحة للجمهور، أو إذا رضي صاحب أو حائز هذه البيانات بهذا التفتيش، أي إذا رضي من يملك السلطة القانونية للكشف عن تلك البيانات، ويقصد به هنا مزود الخدمة، فإن كان للشخص بيانات مخزنة في دولة ما في بريده الإلكتروني مثلا، فإنه يجوز تفتيشها إذا قبل مزود الخدمة في هذه الدولة بذلك.[3]

[1] سامح أحمد، المرجع السابق، ص258.

[2] الغافري، المرجع السابق، ص485.

[3] سامح أحمد، المرجع السابق، ص259.

وقد أجازت م17-2/1 من قانون الأمن الداخلي الفرنسي سالف الذكر لمأموري الضبط القضائي القيام بتفتيش الأنظمة المتصلة حتى ولو تواجدت خارج الإقليم الفرنسي، مع مراعاة الالتزامات الدولية.

ج- شروط التفتيش.

للتفتيش بصفة عامة شروط موضوعية وأخرى شكلية.

- **الشروط الموضوعية للتفتيش.**

سبق القول بأن التفتيش إجراء خطير يمس الحياة الشخصية للأفراد، لذلك أحاطته التشريعات الإجرائية بضوابط معينة، حيث وضعت له شروطا موضوعية وأخرى شكلية.

بخصوص الشروط الموضوعية لتفتيش جهاز الحاسب الآلي ومن هو في حكمه، فيقصد بها الضوابط المطلوبة لإجراء تفتيش صحيح، ويمكن حصرها في ثلاثة شروط رئيسة هي السبب، المحل، والسلطة المختصة للقيام بالتفتيش.

فسبب التفتيش في البيئة الإلكترونية هو السعي نحو الحصول على دليل من أجل الوصول إلى اكتشاف الحقيقة، ويقتضي ذلك أن تقع جريمة من جرائم التجارة الإلكترونية كالمساس بأنظمة المعالجة الآلية للمعطيات، أو الاستعمال غير المشروع لبطاقات الائتمان، أو التعدي على البيانات الشخصية، وغيرها من الجرائم المدروسة عند التطرق للجانب الموضوعي الخاص بالجرائم الواقعة على التجارة الإلكترونية، ويشترط أن تشكل هذه الجرائم جنحا أو جنايات، فالمخالفات البسيطة تستبعد من نطاق التفتيش لتفاهتها، علما أن معظم الجرائم الواقعة على التجارة الإلكترونية عبارة عن جنح، كما ينبغي أن تتوافر في حق من يراد تفتيش شخصه أو مسكنه دلائل قوية،[1] تدعو للاعتقاد أنه مساهم في الجريمة الإلكترونية، سواء أكانت المساهمة أصلية أم تبعية، أو توافر أمارات قوية أو قرائن

[1] لم تتطرق القوانين إلى تعريف المراد بالدلائل القوية، إلا أن الفقه حاول إجلاء الغموض عنها، ومن ذلك تعريفها بأنها: مجموعة من الوقائع الظاهرة والملموسة التي يستنتج منها أن شخصا معينا هو مرتكب الجريمة. وفي مجال الجرائم الإلكترونية فيقصد بالدلائل القوية أو الكافية مجموعة المظاهر أو الأمارات المعينة القائمة على العقل والمنطق والخبرة الفنية والحرفية للقائم بالتفتيش، والتي تؤيد نسبة ارتكاب الجريمة الالكترونية إلى شخص معين، سواء أكان فاعلا أم شريكا، ومن أمثلتها ارتباط عنوان انترنت بروتوكول والخاص بجهاز الحاسب الذ يحوي صورا فاضحة مثلا مع رقم حساب المتهم لدى مزود الخدمات، ووجود رقمين للهاتف لديه يستخدمان لذلك. يراجع كل من: عائشة بن قارة، المرجع السابق، ص102، وكذا شيماء عبد الغني، المرجع السابق، ص282.

على وجود بيانات أو معدات معلوماتية تفيد في كشف الحقيقة لدى المشتبه فيه أو غيره.[1] وقد حددت المادة الرابعة من القانون 09-04 سالف الذكر الحالات التي تجيز تفتيش المنظومة المعلوماتية منها مقتضيات التحريات والتحقيقات القضائية عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى التفتيش، وكذا في إطار تنفيذ المساعدة القضائية الدولية المتبادلة.

أما محل التفتيش فهو المستودع الذي يُحتفظ فيه بالأشياء المادية التي تتضمن الأسرار؛ ومحل التفتيش في الجرائم الإلكترونية هو الحاسب الآلي أو أي جهاز آخر يقوم مقامه، وكذا الشبكة بكل ملحقاتها، أما فيما يخص السلطة المختصة بالتفتيش فإن الأصل أن يقوم قاضي التحقيق بالتفتيش (الجزائر)، أو النيابة العامة (مصر)، إلا أنه يجوز لضابط الشرطة القضائية القيام بذلك استثناء في حالة التلبس، وكذا في حالة الانتداب حسب القواعد العامة، ويجب أن يحدد في إذن الانتداب بالتفتيش المكانُ المراد تفتيشه، والشخص والأشياء المراد تفتيشها، فلا بد من التحديد لتجنب التفتيش الاستكشافي، بحيث لا يكون للضابط المنتدب أية سلطة تقديرية في ذلك، إلا أن هناك صعوبة في احترام هذا الشرط عمليا، نظرا للطبيعة الخاصة لأجهزة الحاسب الآلي التي تحوي عددا كبيرا من الملفات، كما أن أسماء هذه الملفات لا تدل بالضرورة على مسمياتها، فمن الوارد جدا أن يعمد المتهم إلى وضع أسماء مستعارة لملفات تحوي مواد غير مشروعة.

وقد أثيرت بعض الأسئلة بخصوص تفتيش أجهزة الحاسب الآلي منها: هل يعتبر كل ملف من ملفات الحاسب الآلي المراد تفتيشه صندوقا مغلقا يحتاج كل واحد منها إلى إذن قضائي خاص؟ أم أن إذنا واحدا يكفي لتفتيشها كلها؟

تضاربت أحكام القضاء الأمريكي بشأن هذه المسألة، حيث اعتبرت بعضها أن القرص الصلب بما يحويه من ملفات وجهاز الحاسب الآلي بما يحويه من ملفات صندوقا مغلقا واحدا، مما يجيز تفتيش الجهاز كله بما فيه من ملفات مختلفة، بناء على إذن تفتيش واحد، وعلى خلاف ذلك اعتبرت أحكام أخرى في القضاء الأمريكي أن كل ملف في جهاز الحاسب الآلي يتطلب إذنا خاصا لتفتيشه،

[1] عائشة بن قارة، المرجع نفسه، ص103.

وبناء عليه اعتبرت كل ملف صندوقا مغلقا؛ وأحكام هذا الاتجاه تعتبر أن جهاز الحاسب الآلي يحوي الكثير من المعلومات المتعلقة بالحياة الخاصة لصاحبه، التي يجب أن تصان من الاعتداء عليها.[1]

غير أن اعتبار كل ملف من ملفات الحاسب الآلي صندوقا مغلقا يستوجب تفتيشه إذنا خاصا، أمر في غاية الصعوبة من الناحية العملية، خاصة مع التطور السريع لتقنيات الحاسب الآلي وخاصة من حيث السعة التي يمكن أن يحويها القرص الصلب، إذ بإمكانه أن يحوي عددا كبيرا جدا من الملفات، وكل ملف يحوي ملفات عديدة بداخله، وإذا أردنا أن نحصي عدد الملفات التي يمكن أن يحويها قرص صلب سعته واحد "تيرا" فقط لوجدناها تفوق المائة ألف، إذا افترضنا أن متوسط سعة الملف 10 ميجا، والحقيقة أن سعة الملف الواحد لا تتعدى الميجا الواحد بل أقل بكثير، مما يجعل عدد الملفات قد يصل إلى مئات الآلاف، بل الملايين، فهل يعقل أن تستصدر مائة ألف أو أكثر من الأذونات لتفتيش جهاز حاسب آلي واحد؟ ولكن من ناحية أخرى لا يستساغ أن يمتد إذن التفتيش ليطال كل ملفات الحاسب، فتستباح بذلك حياة الشخص الفردية دونما مسوغ، وعليه يجب أن يقيد التفتيش للغرض الذي صدر الإذن لأجله، وهو الحصول على أدلة تفيد القضية محل التحقيق، فبمجرد الحصول على هذه الأدلة يتوقف التفتيش، إذ لا داعي للاستمرار فيه حتى وإن كان ذلك سيكشف عن جرائم أخرى، طالما أن الإذن بالتفتيش محدد، غير أنه وتطبيقا للقواعد العامة، إذا صادف المفتش أثناء بحثه عن الدليل بصدد الجريمة المحقق فيها جريمة أو أكثر عرضية مثل حيازة صور فاضحة فإن أدلة الإدانة بهذه الجريمة صحيحة ولا يشوبها البطلان.[2]

- **الشروط الشكلية للتفتيش.**

التفتيش بصفة عامة لابد له من شروط شكلية بالإضافة إلى الشروط الموضوعية، حتى يتم صحيحا ولا يعتريه البطلان، وللمحافظة على الحريات الشخصية من التعسف في استخدام السلطة، ومن هذه الإجراءات الشكلية ضرورة حضور بعض الأشخاص أثناء إجراء تفتيش المساكن ومن في حكمها، ويعتبر هذا الشرط من أهم الشروط الشكلية التي يتطلبها القانون لإجراء التفتيش، لذا ينص كل من المشرع الجزائري والمشرع الفرنسي على ضرورة حضور شاهدين، سواء أتم التفتيش بمعرفة قاضي التحقيق أم ضابط الشرطة القضائية، إذ وحسب نص م45 ق إ ج التي تقابلها م56 ق

[1] عائشة بن قارة، المرجع السابق، ص106.

[2] أسامة قايد، المرجع السابق، ص454.

إ ج ف فلا بد من حصول التفتيش بحضور المتهم، فإذا لم يستطع الحضور وقت إجراء التفتيش كان عليه بتعيين ممثل له، فإن امتنع أو كان هاربا، أجرى ضابط الشرطة القضائية التفتيش بحضور شاهدين من غير الموظفين الخاضعين لسلطته؛ غير أن الفقرة الأخيرة من م45 ق إ ج سالفة الذكر،[1] استبعدت بصريح العبارة ضمانة حضور الأشخاص المذكورين آنفا إذا تعلق الأمر بجريمة المساس بأنظمة المعالجة الآلية للمعطيات وبعض الجرائم الأخرى،[2] وعليه يجوز التفتيش في هذه الجرائم دونما حاجة لحضور الأشخاص المذكورين أعلاه، ولعل ذلك مرده إلى الطبيعة الخاصة لهذه الجرائم التي تحتاج من أجل الكشف عن الأدلة المتعلقة بها إلى السرعة في التنفيذ، والسرية حتى لا يقوم المجرمون بمحو أو طمس أدلة الإدانة؛ كما أن هذه الضمانة بدأت تتضاءل أهميتها في الدول التي تأخذ بإجراء التفتيش عن بعد،[3] ومنها الجزائر، بحيث أجاز القانون 09-04 في م5 منه الدخول بغرض التفتيش ولو عن بعد إلى منظومة معلوماتية أو جزء منها، والمعطيات المعلوماتية المخزنة فيها، وكذا إلى منظومة التخزين المعلوماتية.

من الشروط الشكلية للتفتيش أيضا إجراؤه في ميقات زمني محدد، حرصا على الحريات الشخصية للأفراد وحرمة مساكنهم، لذلك حظر المشرع الجزائري تفتيش المنازل ومن في حكمها في أوقات معينة حيث أجازه فقط من الساعة الخامسة صباحا إلى الساعة الثامنة مساء (م1/47 ق إ ج)، وكذا فعل المشرع الفرنسي الذي أجاز التفتيش من الساعة السادسة صباحا إلى الساعة التاسعة مساء (م59 ق إ ج ف)، أما المشرع المصري فقد ترك تحديد الوقت للقائم بالتفتيش، ومن ثم يجوز له القيام به في كل الأوقات وعلى مدار 24 ساعة في اليوم، وهو مسلك خطير فيه خشية مساس بحقوق الأفراد الشخصية.

وهناك حالات استثنائية نص عليها المشرع الجزائري يجوز فيها إجراء التفتيش ليلا ونهارا.[4] وحسب نص م3/47 ق إ ج،[5] فإنه يجوز لقاضي التحقيق القيام بأية عملية تفتيش أو حجز ليلا ونهارا...إذا تعلق الأمر ببعض الجرائم، ومنها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، ولعل

---

[1] عدلت م45 ق إ ج بالقانون 06-22 المؤرخ في 2006/12/20، ج ر 84، ص6.

[2] هي جرائم المخدرات، والجريمة المنظمة عبر الحدود الوطنية، وجرائم تبييض الأموال وتمويل الإرهاب، والجرائم المتعلقة بالتشريع الخاص بالصرف.

[3] عائشة بن قارة، المرجع السابق، ص109.

[4] م2/47 ق إ ج.

[5] المعدلة بالقانون 06-22 المؤرخ في 2006/12/20، ج ر84، ص6.

الأمر راجع إلى خصوصية هذه الجرائم التي لا تحتمل تأخير التفتيش بصددها، أما التشريعات التي لم تنص صراحة على مواعيد خاصة لإجراء التفتيش، فلا مناص من التقيد بالقواعد العامة التي تحدد المواقيت الزمنية لإجراء التفتيش في الجرائم الأخرى.

يجب تحرير محضر لإثبات ما تم من إجراءات، وما أسفرت عنه عملية التفتيش من نتائج، ولم يتطلب القانون شكلا خاصا في محضر التفتيش، وبخصوص الجرائم الإلكترونية فمن المحبذ أن يكون رفقة القائم بالتفتيش شخص متخصص في تقنية المعلومات ليساعده على صياغة مسودة محضر التفتيش،[1] بحيث يتم تغطية كل الجوانب الفنية في عملية التفتيش، بالإضافة إلى المحافظة على الأدلة المتحصل عليها، وحمايتها من كل تلف أو مسح أو تحريف.[2]

ويثور التساؤل حول شبكة الانترنت، هل يجوز تفتيشها دون إذن؟

الانترنت شبكة عالمية مفتوحة ومتاحة للجميع، لذا يجوز الدخول إليها والإطلاع على البيانات المتاحة للجمهور دون حاجة للحصول على إذن بالتفتيش، أما إذا كانت هذه البيانات مخزنة لدى مزودي خدمات متواجدين في إقليم دولة أخرى، فإنه واحتراما لسيادة هذه الدولة يجب اللجوء إلى طلب المساعدة القضائية من الدولة المتواجد بها مزودو الخدمات المخزنة لديهم البيانات المراد تفتيشها.[3]

ووفقا للقواعد العامة، فإن تفتيش مواقع الانترنت لا تسري عليها قواعد وأحكام تفتيش المساكن، وبالتالي لا تتوافر لها الحماية المقررة في التشريعات المختلفة للمساكن ومن ضمنها الحصول على إذن التفتيش.[4]

---

[1] عائشة بن قارة، المرجع السابق، ص113.

[2] خالد ممدوح إبراهيم، المرجع السابق، ص225.

[3] سامح أحمد، المرجع السابق، ص262.

[4] سامح أحمد، المرجع السابق، ص262.

د- أسلوب تفتيش نظم الحاسب الآلي.[1]

جرائم تقنية المعلومات لها طبيعة خاصة، لذا يتوجب التعامل معها أثناء التفتيش بطرق خاصة تتلاءم وطبيعتها، بأن تكون هناك مرونة ولياقة لا تتعارض مع الطبيعة الخاصة لهذه الجرائم وتخدم روح العدالة.

التفتيش عن الملفات الموجودة في جهاز الحاسب الآلي من الأمور المعقدة، فالملفات يمكن تخزينها في قرص لين أو بطاقة ذاكرة أو غيرها أو عناوين مخبأة في الحاسب المتنقل الخاص بالمشتبه فيه، أو على خادم بعيد جدا وخارج حدود الدولة، كما يمكن تشفير الملفات، مع وضع عناوين مضللة لها وتخزينها في شكل ملفات غير تقليدية، أو أن يتم خلطها مع آلاف بل ملايين الملفات التي ليس لها علاقة بالموضوع، أو ملفات غير سيئة أو ضارة وتكون محمية...لذا فإن تفتيش نظم الحاسب الآلي هو للفن أقرب منه للعلم.

يمكن للقائمين بالتفتيش توسيع احتمالية نجاح العملية باتباع الخطوات التالية:

- تجميع فريق عمل، يكون من ضمنه الخبير الفني قبل القيام بالتفتيش.
- التعرف قدر المستطاع على نظم الحاسب الآلي المراد تفتيشها قبل وضع خطة التفتيش أو طلب الإذن.
- وضع خطة لتنفيذ التفتيش (الخطة أ) ووضع خطة بديلة (الخطة ب)، مبنية على المعلومات التي جمعت عن النظام المراد تفتيشه.
- إعطاء مسودة إذن التفتيش عناية خاصة من حيث اشتمالها على وصف لمحل التفتيش، والأشياء المراد ضبطها بدقة وواقعية، مع شرح إستراتيجية التفتيش الممكنة.

3- الضبط.

الهدف من التفتيش هو ضبط الأشياء المتعلقة بالجريمة تفيد في التحقيق الجاري بشأنها، سواء أكانت هذه الأشياء أدوات استعملت في ارتكاب الجريمة، أو ناتجة عنها أو غير ذلك مما يفيد في كشف الحقيقة؛ والضبط من حيث طبيعته القانونية قد يكون من إجراءات الاستدلال أو من

[1] خالد ممدوح إبراهيم، المرجع السابق، ص225-227.

إجراءات التحقيق،[1] والضبط بطبيعته لا يرد إلا على الأشياء دون الأشخاص، سواء أكانت منقولا أم عقارا؛ والقاعدة أن الضبط لا يرد إلا على شيء مادي، أما الأشياء المعنوية فلا تصلح بطبيعتها للضبط،[2] لذلك يختلف الضبط في الجريمة الإلكترونية عن الضبط في غيرها من الجرائم من حيث المحل، فمحل الضبط في الجرائم الإلكترونية البيانات والمراسلات والاتصالات الإلكترونية،[3] بالإضافة إلى المكونات المادية للحاسب الآلي أو الهاتف النقال...

الأدلة المادية التي يجوز ضبطها في الجريمة المعلوماتية والتي لها قيمة خاصة في إثبات الجرائم الواقعة على التجارة الإلكترونية هي:

– الأوراق التي قد يخلفها الجناة وراءهم، وهو أربعة أنواع: أوراق تحضيرية يتم إعدادها بخط اليد كمسودة، أو تصور للعملية المراد القيام بها، أوراق تالفة تتم طباعتها للتأكد، ثم ترمى في سلة المهملات، أوراق أصلية يتم طباعتها والاحتفاظ بها كمرجع، أو لأغراض تنفيذ الجريمة، وأوراق أساسية وقانونية محفوظة في الملفات العادية أو دفاتر الحسابات، لها علاقة بالجريمة، خاصة عند تزوير بياناتها.

– جهاز الحاسب الآلي أو أي جهاز يقوم مقامه، وملحقاته، وذلك بالاستعانة بأهل الخبرة الفنية لتمييزه عن الأجهزة الأخرى وتحديد طريقة التعامل معه في حالة ضبطه.

– لوحة المفاتيح، الشاشة، نظام الفأرة، الطابعة، الرسم، وحدات التخزين المختلفة، البرامج اللينة البطاقات الممغنطة وأدلة الاستعمال المصاحبة للحاسب الآلي...

لا يثور بالنسبة لهذه المكونات المادية أي إشكال، إذ تطبق عليها القواعد العامة المتعلقة بضبط الأشياء؛ غير أن طبيعة الجرائم الإلكترونية تستدعي ضبط البيانات الإلكترونية، وهنا يثور الإشكال حول مدى صلاحيتها لأن تكون محلا للضبط، وهو الإشكال ذاته الذي طرح بصدد التفتيش، وانقسم الفقه حوله، إلا أن الراجح أنه يجوز تفتيشها وبالتالي ضبطها، والسؤال هنا: كيف يتم ضبطها من الناحية الفنية؟ هناك أساليب متعددة تضبط بها البيانات المعالجة آليا منها أسلوب النسخ، عن طريق برامج متخصصة في النسخ، وأسلوب تجميد التعامل بالحاسب الآلي أو إحدى

[1] علي عدنان الفيل، إجراءات التحقيق الابتدائي في الجريمة المعلوماتية، المجلة القانونية التونسية، مركز النشر الجامعي، تونس 2009، ص59.

[2] الفيل، المرجع السابق، ص60.

[3] عائشة بن قارة، المرجع السابق، ص114.

القطع المكونة له؛ ولقد نصت م19 من اتفاقية بودابست لسنة 2001 على: "من سلطة كل دولة طرف أن تتخذ الإجراءات التالية: أن تضبط نظام الحاسب الآلي أو جزء منه... وأن تحافظ على سلامة تلك المعلومات المخزنة"، ونص المشرع الفرنسي في م76-1 فقرة 3 من القانون رقم 239 لسنة 2003 على أن البيانات التي يتم الحصول عليها من جراء تفتيش النظام المعلوماتي يتعين نسخها على دعامات يتم تحريزها، الأمر ذاته نصت عليه م6 من القانون 09-04 سالف الذكر "...يتم نسخ المعطيات محل البحث والمعطيات اللازمة لفهمها على دعامة تخزين إلكترونية تكون قابلة للحجز والوضع في أحراز وفقا للقواعد المقررة في قانون الإجراءات الجزائية" مع ضرورة السهر على سلامة المعطيات، وتثور المشكلة عندما يلزم ضبط النظام أو الشبكة بالكامل، لاحتوائها على عناصر غير قابلة للفصل، هنا يتم إعمال مبدأ التناسب، أو بتعبير آخر مبدأ تغليب المصالح أو المفاضلة بين المصالح، حيث يتم التوازن بين مصلحتين، مصلحة المجتمع في كشف الحقيقة، ومصلحة صاحب النظام في تسيير أعماله، وعدم تفويت فرص الربح، لذلك قضت المحكمة الفدرالية الألمانية بإلغاء قرار الضبط الذي ورد على 220 قرصا بالإضافة إلى الوحدة المركزية للحاسب الآلي، لإخلاله بمبدأ التناسب.[1]

وخشية محو أو إتلاف أو ضياع الأدلة أعطت بعض التشريعات ومنها م88 من قانون تحقيق الجنايات البلجيكي، لقاضي التحقيق سلطة التحفظ عليها إن وجدت على الإقليم البلجيكي، أو أن يطلب من السلطات الأجنبية نسخة من البيانات محل الجريمة إن وجدت لدى دولة أجنبية.[2]

يواجه إجراء ضبط البيانات المعالجة إلكترونيا صعوبات منها:

– حجم الشبكة التي تحتوي على المعلومات المعالجة إلكترونيا والمطلوب ضبطها، من ذلك البحث في نظام إلكتروني لشركة متعددة الجنسيات، والحل هو إعمال مبدأ التناسب.

– وجود هذه البيانات في شبكات أو أجهزة تابعة لدولة أجنبية.

– يمثل التفتيش والضبط في بعض الأحيان اعتداء على حقوق الغير، أو على حرمة حياته الخاصة، لذا وجب اتخاذ كافة الضمانات للحفاظ على هذه الحقوق والحريات.

[1] عائشة بن قارة، المرجع السابق، ص116.

[2] الفيل، المرجع السابق، ص64.

لضمان الحفاظ على البيانات محل البحث، ومقارنتها بالنسخة المخرجة من الجهاز في حالة إنكارها من المتهم، فقد أعطى القانون البلجيكي بموجب م29 مكرر3 للنيابة العامة سلطة الأمر بغلق هذه المعطيات (Blocage de données) لمنع الوصول إليها، أو إلى النسخة المستخرجة منها الموجودة لدى من يستعملون النظام.[1]

تطرق المشرع الجزائري من خلال م3/6 من القانون 09-04 سالف الذكر إلى جواز استعمال الوسائل التقنية الضرورية لتشكيل أو إعادة تشكيل المعطيات محل الضبط، بغية جعلها قابلة للاستغلال لأغراض التحقيق طالما لم يؤد ذلك إلى المساس بسلامتها، وإذا استحال الضبط أو الحجز كما أسماه المشرع الجزائري لأسباب تقنية، تعين على القائم بالتفتيش استعمال التقنيات المناسبة لمنع الوصول إلى المعطيات التي تحتويها المنظومة المعلوماتية، أو إلى نسخها، الموضوعة تحت تصرف الأشخاص المرخص لهم باستعمال هذه المنظومة (م07)، ويجوز للسلطة التي تباشر التفتيش الأمر باتخاذ الإجراءات اللازمة لمنع الاطلاع على المعطيات التي يشكل محتواها جريمة، عن طريق تكليف أي شخص مؤهل باستعمال التقنية المناسبة لذلك.

4- الشهادة في الجرائم الإلكترونية.

الشهادة هي الأقوال التي يدلي بها غير الخصوم أمام سلطة التحقيق بشأن جريمة وقعت، سواء تعلقت بثبوت الجريمة وظروف ارتكابها وإسنادها إلى متهم، أو ببراءته منها، وللشهادة أهمية بالغة في الكشف عن الحقيقة لذلك جاء مبدأ عدم جواز رد الشهود، وسماع قاضي التحقيق للشهود يخضع من الناحية القانونية للقواعد العامة؛[2] والشاهد في الجريمة المعلوماتية هو الشخص الفني صاحب الخبرة والمتخصص في تقنية المعلومات، صاحب الكفاءة في التعامل مع نظام المعالجة الآلية للمعطيات، ويجوز القول أن الشاهد المعلوماتي ينحصر في عدة طوائف هي: مشغلو الحاسب الآلي، خبراء البرمجة، المحللون، مهندسو الصيانة والاتصالات، ومديرو النظم.[3]

على الشاهد المعلوماتي الالتزام بالإعلام، ومعنى ذلك أنه متى كان حائزا لمعلومات جوهرية لازمة للولوج إلى نظام المعالجة الآلية للمعطيات، فإنه يكون مطالبا بإعلام سلطات التحقيق

---

[1] الفيل، المرجع السابق ص64.

[2] المرجع نفسه، ص66.

[3] بيومي حجازي، الجوانب الإجرائية، المرجع السابق، ص612-613.

على سبيل الإلزام، وإلا تعرض للعقوبات المقررة للامتناع عن الشهادة، وذلك في غير الأحوال التي يجيز له القانون فيها ذلك.[1]

والسؤال المطروح: هل يلزم الشاهد المعلوماتي بطبع الملفات والإفصاح عن كلمات المرور والشفرات؟

ظهر اتجاهان بهذا الشأن: الاتجاه الأول يرى بأن الشاهد غير مجبر أن يقوم بطبع ملف البيانات، أو الإفصاح عن كلمة المرور أو الشفرات الخاصة بالبرامج المختلفة، وممن يعتنقون هذا الرأي الفقهاء في ألمانيا وتركيا؛ أما الاتجاه الثاني فيرى أن القيام بالطبع والإفصاح من التزامات الشاهد، وتبنى هذا الرأي جانب من الفقه الفرنسي الذي يرى أن الإخلال بهذا الالتزام يعاقب عليه في مرحلة التحقيق والمحاكمة دون مرحلة الاستدلال، أما في اليونان فيجوز الحصول من القائم على تشغيل نظام الحاسب الآلي على كلمة المرور السرية للولوج في نظام المعلومات، كما يجوز الحصول منه على بعض الإيضاحات الخاصة بنظامه الأمني، بيد أنه ليس على الشاهد أي التزام بالنسبة لطباعة ملفات معطيات مخزنة في ذاكرة الحاسب الآلي، لسبب بسيط أن الشاهد ملزم بالشهادة على معلومات حازها فعلا، وليس الكشف عن معلومات جديدة.[2]

وقد تلجأ بعض الدول إلى وسائل الضغط على الشهود لحملهم على الإفصاح عن كلمة السر أو الشفرة، تحت طائلة العقوبات، إما باعتباره شريكا في الجريمة موضوع المحاكمة أو على أساس شهادة الزور.[3]

ونرى أن يكون تدخل المشرع بنص خاص وصريح يحدد التزامات الشاهد المعلوماتي، وعقوبة الإخلال بها.

5- الخبرة الفنية.

الخبرة القضائية[1] وسيلة قررها المشرع لمساعدة القاضي أو المحقق في تقدير المسائل التي يحتاج إثباتها إلى معرفة علمية أو فنية خاصة، بالرجوع إلى الأشخاص ذوي المعارف الخاصة

[1] بيومي حجازي، المرجع السابق، ص614.

[2] الفيل، المرجع السابق، ص69.

[3] عائشة بن قارة، المرجع السابق، ص137.

والكفاءات العالية، وهم الخبراء المتخصصون في علم من العلوم أو فن من الفنون، فالخبرة ما هي إلا وسيلة من وسائل الإثبات تنصب على الواقعة المراد إثباتها للتعرف على حقيقتها من الناحية الفنية.[2]

أما الخبير فقد يكون موظفا عاما مثل الطبيب الشرعي وخبير البصمات والمهندس الفني، وقد لا يكون كذلك مثل أصحاب الحرف، وقد يكون من الإطارات الخاصة مثل بعض أساتذة الجامعات في كل التخصصات، ويشترط في الخبير الجمع بين العلم ذي الاختصاص والخبرة العملية.[3]

وإذا كانت الخبرة ذات أهمية كبيرة في إثبات الجرائم التقليدية، فإن أهميتها تتعاظم بالنسبة للجرائم الإلكترونية عامة، وجرائم التجارة الإلكترونية على وجه الخصوص، حيث تتعلق بمسائل فنية غاية في التعقيد، لا يستطيع كشف حلها سوى متخصص متمرس متميز في مجال تخصصه،[4] فالعلوم والتقنيات المتصلة بالمعلوماتية في تطور وتغير سريع ومستمر لدرجة يصعب معها حتى على المتخصصين تتبعها واستيعابها، لذلك يلجأ المحققون والقضاة إلى أكثر من خبير؛ ورغم أن ندب الخبراء جوازي للمحقق أو القاضي، فإن الاستعانة بهم في المسائل الفنية البحتة ومنها الجرائم الإلكترونية، التي لا يستطيع القاضي أن يقطع فيها برأي دون الرجوع إلى أهل الخبرة واجب، فإذا تصدى القاضي للقضية دون استطلاع أهل الخبرة كان حكمه معيبا مستوجبا للنقض، وهذا المبدأ أقرته محكمة النقض المصرية.[5] غير أن هذا لا يعني أن القاضي يجب عليه الأخذ برأي الخبير، فهو غير ملزم بذلك، وله مطلق الحرية في تقديره، وله أن يأمر بإجراء خبرة تكميلية أو خبرة مضادة أو مقابلة، خاصة في حال تعارض النتائج التي توصل لها الخبير مع غيره من الخبراء أو مع شهادة أحد الشهود، لكن لا يجوز للقاضي تفنيد النتائج الفنية التي توصل لها الخبير إلا بأسانيد فنية.[6]

من الناحية العملية يبني القاضي قناعته بناء على ما خلص إليه الخبير في تقرير خبرته.

---

[1] أضاف المشرع الجزائري فصلا سادسا إلى الأمر 66-155، بموجب الأمر 15-02 سالف الذكر، تضمن هذا الفصل عشر مواد: من م65 مكرر 19 إلى م65 مكرر28، تحت عنوان حماية الشهود والخبراء والضحايا، تضمن إجراءات من شأنها توفير حماية أكبر لهؤلاء.

[2] سهام لمريني، الخبرة القضائية في المواد الجزائية، أطروحة دكتوراه في الحقوق، جامعة أبي بكر بلقايد، تلمسان 2014/2013، ص76.

[3] خالد ممدوح إبراهيم، المرجع السابق، ص285.

[4] عائشة بن قارة، المرجع السابق، ص139.

[5] الفيل، المرجع السابق، ص37.

[6] عائشة بن قارة، المرجع السابق، ص146.

الخبرة الفنية في أغلب التشريعات تخضع للقواعد العامة شأنها في ذلك شأن الخبرة المتعلقة بالجرائم التقليدية سواء من حيث اختيار الخبراء أو ردهم، أو حق الخصوم في الاستعانة بخبير، إلا أن هناك بعض التشريعات نصت على الخبرة في مجال الجرائم الإلكترونية مثل القانون البلجيكي الصادر في 23 /2000/11 حيث نصت م88 منه على أنه: "يجوز لقاضي التحقيق، وللشرطة القضائية أن يستعينا بخبير ليقدم بطريقة مفهومة المعلومات اللازمة عن كيفية تشغيل النظام، وكيفية الدخول فيه، أو الدخول للبيانات المخزنة أو المعالجة أو المنقولة بواسطته، ويعطي القانون كذلك لسلطة التحقيق أن تطلب من الخبير تشغيل النظام، أو البحث فيه، أو عمل نسخة من البيانات المطلوبة للتحقيق، أو سحب البيانات المخزنة أو المحولة أو المنقولة، على أن يتم ذلك بالطريقة التي تريدها جهة التحقيق".

وفقا للقانون البلجيكي المذكور فإن الالتزام بتشغيل النظام واستخراج المعطيات المطلوبة منه، يرجع بصفة أصلية إلى قاضي التحقيق، ويجوز ذلك للنيابة العامة استثناء في حالة التلبس، أو عند الرضاء بعملية التفتيش، فمهمة الخبير حسب النص القانوني البلجيكي تتمثل في تشغيل النظام، وكذا تقديم المعطيات المطلوبة، حسب الطريقة التي تريدها جهة التحقيق (على ورق أو أقراص...)؛ والتزام الخبير هو التزام ببذل عناية لا بتحقيق نتيجة، ولا تثور مسؤوليته الجزائية إلا إذا رفض القيام بالمهمة المكلف بها، أو أتلف عمدا المعطيات المطلوب منه التعامل معها أو حفظها أو قام بإفشاء سر من أسرار مهنته.[1]

تساعد الخبرة في الجرائم المعلوماتية على الوسائل التالية:[2]

- الكشف عن الدليل الإلكتروني، والتأكد من عدم العبث به أو تعديله.
- إجراء الاختبارات التكنولوجية والعلمية على الدليل لاختباره والتحقق من أصالته ومصدره كدليل، يجوز تقديمه لأجهزة العدالة.
- تحديد الخصائص الفريدة للدليل الإلكتروني.
- إصلاح الدليل وإعادة تجميعه من المكونات المادية للحاسب الآلي.
- عمل نسخة أصلية من الدليل الإلكتروني للتأكد من عدم وجود معلومات مفقودة أثناء عملية استخلاص الدليل.

[1] الفيل، المرجع السابق، ص40.

[2] خالد ممدوح إبراهيم، المرجع السابق، ص302.

- جمع الآثار المعلوماتية الرقمية التي قد تكون تبدلت خلال الشبكة المعلوماتية.
- تحريز الدليل الإلكتروني لتقديمه ضمن الأدلة المقدمة في الدعوى.

ثانيا: الإجراءات المستحدثة في تحقيق الجرائم الإلكترونية.

فرضت طبيعة الجرائم الإلكترونية نفسها على المشرع في القانون المقارن، أن يستحدث إجراءات جديدة للتصدي لهذا النوع من الجرائم، ولقد تطرق المشرع الجزائري في قانون الإجراءات الجزائية والقانون 09-04 إلى بعض هذه الإجراءات.

1- عملية التسرب.

التسرب لغة يعني الدخول خفية، أو الولوج بطريقة تسللية إلى مكان ما، أو جماعة معينة، وجعلهم يعتقدون بأن المتسرب ليس غريبا عنهم، بل واحدا منهم، أما اصطلاحا فللتسرب عدة مرادفات كالتوغل أو الاختراق؛ وعملية التسرب عملية تقنية، يُتمكن من خلالها الدخول إلى وسط مغلق كجماعة إجرامية إرهابية أو شبكة تتاجر في مواد ممنوعة كالمخدرات أو الأسلحة، فعملية التسرب تقوم على فكرة إقحام عنصر أجنبي عن الجماعة المراد اختراقها داخلها ليكون عينا عليها يرقب أعمالها ويرصد تصرفاتها، وهذا ما يطلق عليه أيضا "الزرع"، أي زرع أحد ضباط أو أعوان الضبطية القضائية ممن تتوفر فيهم بعض المواصفات الخاصة وسط مجموعة إجرامية، بقصد مراقبتها من الداخل، ومعرفة الإمكانات المادية والبشرية والتنظيمية للمجموعة من أساليب عمل ووسائل اتصال وتنقل...حتى تتمكن المصالح الأمنية من مكافحة إجرامهم وتقديمهم للعدالة، وإثبات التهم عليهم.[1]

أدرج المشرع الجزائري عملية التسرب بموجب القانون رقم 06-22 المؤرخ في 2006/12/20 المعدل والمتمم لقانون الإجراءات الجزائية، أفرد الفصل الخامس منه تحت عنوان "في التسرب" وتضمن ثماني مواد (65 مكرر11 – 65 مكرر18)، تناول من خلالها تحديد مفهوم عملية التسرب، شروط إجرائها، مبرراتها، والحماية الجزائية للمتسرب.

حسب م65 مكرر12 من ق ا ج فإن التسرب معناه: قيام ضابط أو عون الشرطة القضائية تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية، بمراقبة الأشخاص المشتبه

[1] أعمر قادري، أطر التحقيق، دار هومة، الجزائر 2013، ص72.

في ارتكابهم جناية أو جنحة بإيهامهم أنه فاعل معهم أو شريك أو خاف. ويلجأ إلى هذا الإجراء عادة عندما تقتضي ذلك عملية التحري أو التحقيق في إحدى الجرائم المذكورة في م65 مكرر ومنها **الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات**.

يرى جانب من الفقه ضرورة الالتزام بحرفية النص القانوني فيما يخص شخص المتسرب، الذي يجب أن يكون من ضباط أو أعوان الشرطة القضائية دون غيرهم، إلا أن هناك رأيا فقهيا آخر، لا يرى مانعا من التوسع في فهم وتفسير النص، ويجيز تبعا لذلك أن يكون المتسرب أي شخص تتوافر فيه المواصفات حتى وإن كان مواطنا عاديا،[1] ولعل هذا الرأي الأخير أكثر واقعية خاصة فيما يتعلق بالجرائم الإلكترونية التي تتطلب مواصفات فنية في المتسرب قد لا توجد في عون أو ضابط الشرطة القضائية.

ويتصور تجسيد عملية التسرب في الجرائم الإلكترونية في اشتراك ضابط أو عون الشرطة القضائية أو غيرهما في محادثات غرف الدردشة عن اختراق الشبكات أو تقليد المصنفات، فيتخذ المتسرب اسما مستعارا، ويظهر كما لو كان واحدا منهم، ويحاول الاستفادة من مهاراتهم حول كيفية اقتحام "الهاكر" لموقع ما.[2]

لما كان التسرب إجراء غير عادي قد يمس بحرمة الحياة الخاصة للغير، أحاطه المشرع بسياج من الضمانات تتمثل فيما يلي:

- صدور إذن التسرب من وكيل الجمهورية أو قاضي التحقيق، بعد إخطار وكيل الجمهورية.
- وجوب أن يكون الإذن مكتوبا، و مسببا.
- ذكر الجريمة التي تبرر اللجوء إلى هذا الإجراء، وهوية ضابط الشرطة القضائية الذي تتم العملية تحت مسؤوليته.
- تحديد مدة عملية التسرب في الإذن، وحسب القانون لا يجوز أن تتجاوز أربعة أشهر قابلة للتجديد بحسب مقتضيات التحري أو التحقيق ضمن الشروط ذاتها، مع جواز أن يأمر القاضي الذي رخص بإجرائها بوقفها في أي وقت قبل انقضاء المدة المحددة.

---

[1] أعمر قادري، المرجع السابق، ص77.

[2] عائشة بن قارة، المرجع السابق، ص120.

نلحظ مما سبق أن المشرع قد أجاز إسناد مهمة إصدار الإذن لوكيل الجمهورية، وهو جهة اتهام، وما دام المشرع قد أخذ بنظام الفصل بين التحقيق والاتهام، كان من الأفضل أن يقصر صدور الإذن على قاضي التحقيق، هذا من جهة، ومن جهة ثانية يثور التساؤل عن الدور الإيجابي للمتسرب في ارتكاب الجريمة، ضمن ما يسميه الفقه "التحريض البوليسي"، وهو مسلك منتقد فقها،[1] ولكن المشرع قد وضح مهمة المتسرب،ويستشف من النص بأنها لا تهدف إلى التحريض على ارتكاب الجريمة، بل إلى معايشة مرتكبيها عن قرب للكشف عنهم، وتقديمهم للعدالة، وذلك فرق جوهري.

نص المشرع في م65 مكرر14 على أنه يجوز لضباط وأعوان الشرطة القضائية المرخص لهم بإجراء عملية التسرب والأشخاص الذين يسخرون لهذا الغرض القيام بما يلي:

– اقتناء أو حيازة أو نقل أو تسليم أو إعطاء مواد أو أموال أو منتوجات أو وثائق أو معلومات متحصل عليها من ارتكاب الجرائم أو مستعملة في ارتكابها.
– استعمال أو وضع تحت تصرف مرتكبي هذه الجرائم الوسائل ذات الطابع القانوني أو المالي و كذا وسائل النقل أو التخزين أو الإيواء أو الحفظ أو الاتصال.

ومن خلال هذا النص يتضح أن طبيعة هذه الأفعال تستوجب من القائمين بها مشاركة إيجابية، كحيازة متحصلات الجريمة أو وسائل ارتكابها، وهذا النوع من الأفعال يوجب المسؤولية الجزائية، غير أن القانون أعفاهم من المسؤولية بنصه صراحة على ذلك في م65 مكرر14، ونعتقد أن هذا من قبيل التزيد، إذ أن عمل هؤلاء الضباط يدخل ضمن أسباب الإباحة "فيما أذن أو أمر به القانون"، وعليه حتى لو لم يوجد نص خاص فهم غير مسؤولين جزائيا، غير أن تجاوز الغرض المحدد من التسرب هو الذي تتحقق به المسؤولية الجزائية حسب القواعد العامة.

يجب أن تتم عملية التسرب في سرية تامة، لتحقق أهدافها، ولحماية المتسرب من المجرمين، ولذلك نصت م65 مكرر16 وما بعدها على عقوبة الحبس والغرامة لكل من يكشف هوية ضباط أو أعوان الشرطة القضائية، وتشدد العقوبة إذا تسبب الكشف في أعمال عنف أو ضرب أو

[1] عائشة بن قارة، المرجع السابق، ص122.

جرح أحد هؤلاء الأشخاص أو أزواجهم أو أبنائهم أو أصولهم المباشرين، وتشدد العقوبة أكثر في حالة وفاة أحد هؤلاء الأشخاص.

وفي نهاية الفصل الخاص بإجراء التسرب نص المشرع على جواز سماع المتسرب بوصفه شاهدا على العملية (م65 مكرر18).

2- التحفظ العاجل على المعطيات المخزنة.

نصت م16 من اتفاقية بودابست لسنة 2001 على ضرورة أن تأمر كل دولة طرف مزود الخدمة التحفظ العاجل على المعطيات المخزنة بواسطة نظام معلوماتي، خلال مدة 90 يوما كحد أقصى قابلة للتمديد، طالما وجدت أسباب تدعو للاعتقاد أن هذه المعطيات معرضة للفقد أو التغير.

الأمر نفسه نصت عليه م23 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، والتي دعت إلى إلزام من بحيازته أو سيطرته معلومات تقنية المعلومات المخزنة بحفظها وسلامتها لمدة 90 يوما كحد أقصى قابلة للتمديد، بغية تمكين السلطات المختصة بالبحث والتقصي.

التحفظ العاجل إجراء أولي الهدف منه محاولة الاحتفاظ بالبيانات خشية فقدانها، وقد حددت م23 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات بأن الهدف من اتخاذ الإجراء هو تمكين السلطات المختصة بالبحث والتحري، وأفاضت المذكرة التفسيرية لاتفاقية بودابست في الأسباب التي تدعو لاتخاذ هذا الإجراء.[1]

3- حفظ المعطيات المتعلقة بحركة السير.

نصت م11 من من القانون 09-04 سالف الذكر على التزام مقدمي الخدمات بحفظ المعطيات المتعلقة بالسير مدة سنة واحدة ابتداء من تاريخ التسجيل، وهذه المعطيات هي التي تسمح بالتعرف على مستعملي الخدمة، أو التجهيزات الطرفية المستعملة للاتصال، أو الخدمات التكميلية المطلوبة أو المستعملة ومقدميها، أو المرسل إليهم الاتصال وعناوين المواقع المطلع عليها؛ وقد عرفت م2/هـ المعطيات المتعلقة بحركة السير بأنها: "أي معطيات متعلقة بالاتصال عن طريق منظومة

[1] عائشة بن قارة، المرجع السابق، ص159.

معلوماتية، تنتجها هذه الأخيرة باعتبارها جزءا في حلقة اتصالات، توضح مصدر الاتصال، والوجهة المرسل إليها، والطريق الذي يسلكه، ووقت وتاريخ وحجم ومدة الاتصال ونوع الخدمة.

من خلال التعريف يتبين أن المعطيات المتعلقة بالسير لا تتعلق بموضوع الاتصال وما دار فيه، بل بمعلومات حوله دون معرفة محتواه، ولأدل على ذلك أن م11 عندما تطرقت إلى نشاطات الهاتف أوجبت على المتعامل حفظ المعطيات وكذا التي تسمح بالتعرف على مصدر الاتصال وتحديد مكانه، ولم تشر إلى مضمون الاتصال خلافا للحفظ العاجل للمعطيات الذي غرضه حفظ المعطيات للاطلاع عليها كونها مفيدة للتحقيق والتقصي، وقد نصت م1/17 من اتفاقية بودابست على سرعة التحفظ على خط سير المعطيات في فقرتيها أ و ب وبينت أن الهدف من ذلك هو إمكانية تحديد مقدم الخدمة، والمسار الذي تم نقل الاتصال من خلاله.

علاوة على العقوبات الإدارية، رتب المشرع الجزائري مسؤولية جزائية للأشخاص الطبيعيين والمعنويين الذين نتج عن عدم احترامهم الالتزامات المنصوص عليها في هذه المادة (م4/11 من القانون 09-04) عرقلة حسن سير التحريات القضائية، فعاقب الشخص الطبيعي بالحبس من ستة أشهر إلى خمس سنوات، والغرامة من خمسين ألفا إلى خمسمائة ألف دينار، أما الشخص المعنوي فيعاقب حسب القواعد العامة لقانون العقوبات أي بغرامة قدرها 2.5 مليون دينار، مع قيام مسؤولية الشخص الطبيعي الذي تصرف باسم الشخص المعنوي أو لحسابه.

أما المشرع الفرنسي فقد أجاز الاحتفاظ بالمعطيات الخاصة لمدة أقصاها سنة طالما أن مقتضيات البحث والتحقيق والمتابعة القضائية تتطلب ذلك، وإلا وجب مسحها حفاظا على حرمة الحياة الخاصة.[1]

4- الأمر بتقديم بيانات إلكترونية متعلقة بالمشترك.

الأصل أن البيانات الشخصية المتعلقة بمستخدمي الشبكة بيانات تدخل في إطار الحقوق الشخصية التي تحميها الاتفاقيات الدولية والقوانين الوطنية، إلا أن بعض التشريعات المقارنة تسمح لرجال الضبط القضائي أن يأمروا الأشخاص بتسليم ما تحت أيديهم من موضوعات لتقديمها كدليل،

[1] فطيمة بوعناد، مشروعية الدليل الإلكتروني في مجال الإثبات الجنائي، أطروحة دكتوراه في العلوم، تخصص حقوق، فرع علوم جنائية، جامعة الجيلالي ليابس، سيدي بلعباس 2014/2013، ص179.

ومن بينها البيانات المتعلقة بالمشترك التي يحوزها مزود الخدمة، وهو ما يلزمه القانون الفرنسي رقم 719 لسنة 2000 الخاص بحرية الاتصالات في المادة 9/43 منه، وأجاز القانون الأمريكي المعروف بقانون خصوصية الاتصالات الالكترونية "ECPA" لرجال الضبط القضائي الاطلاع على البيانات الموجودة لدى مزودي الخدمات، من خلال تكليف مزود الخدمة بتقديم تلك المعلومات،[1] كما نصت على هذا الأمر م18 من اتفاقية بودابست؛ والمعلومات المطلوب تقديمها ثلاثة أنواع هي: المعلومات الشخصية الخاصة بالمشترك كاسمه وعنوانه ورقم هاتفه، والمعلومات الشخصية الخاصة بالمتعامل مع المشترك، أي كل من يتصل به أو يدخل معه في صفقة، والمعلومات المتعلقة بمحتوى البيانات كمضمون المحادثات والملفات؛ وبناء عليه فإن المشترك في خدمات مزود الخدمات لا يتمتع بالحق في الخصوصية بالنسبة لهذه الأنواع الثلاثة من المعلومات.[2] وقد بينت م3/18 من اتفاقية بودابست المراد من مصطلح "معلومات المشترك" بأنه أية معلومات في صورة بيانات حاسب آلي أو أية صورة أخرى يتم حفظها من جانب مقدم الخدمة، والتي تتعلق بالمشتركين في الخدمات الخاصة به بخلاف خط سير البيانات أو مضمونها...

5- التجميع الفوري لبيانات الحاسب الآلي

نص المشرع الجزائري على تجميع الاتصالات الالكترونية في م3 من القانون 09-04 سالف الذكر "...وتجميع وتسجيل محتواها..."، كما نصت على التجميع الفوري م20 اتفاقية بودابست، ويختلف هذا الإجراء عن إجراء التحفظ العاجل أو السريع الذي تطرقت إليه م16 من الاتفاقية المذكورة، في أن البيانات في حالة التحفظ مخزنة لدى مقدم الخدمة بالنظام المعلوماتي للحاسب الآلي أو أحد ملحقاته، بينما في حالة التجميع فالبيانات ليست مخزنة، وتهدف هذه الإجراءات إلى جمعها أو تخزينها وقت مباشرة الاتصال، لذا فهو يحتاج إلى وسائل تقنية حديثة قد لا تتوافر لدى السلطة المختصة، أو قد لا يكون بمقدورها القيام به، ولذا أسندت الاتفاقية القيام بإجراء التجميع أو التسجيل للسلطة المختصة في الدول لتقوم به بنفسها أو من خلال مقدم الخدمة أو بمساعدته.[3] وهذا ما تطرقت إليه أيضا م1/29 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.

---

[1] عائشة بن قارة، المرجع السابق، ص161.

[2] شيماء عبد الغني، المرجع السابق، ص216.

[3] فطيمة بوعناد، المرجع السابق، ص187.

6- مراقبة الاتصالات الإلكترونية.

نص المشرع الجزائري في م3 من القانون 09-04 سالف الذكر على جواز وضع ترتيبات تقنية لمراقبة الاتصالات الالكترونية إذا اقتضت متطلبات حماية النظام العام، أو مستلزمات التحريات أو التحقيقات القضائية الجارية ذلك.

يقصد بهذا الإجراء مراقبة الاتصالات الالكترونية أثناء بثها، وليس الحصول على اتصالات إلكترونية مخزنة، ولا يشترط تجميع هذه الاتصالات.

يثور التساؤل بهذا الخصوص حول طبيعة البريد الإلكتروني غير المفتوح والمنتظر في صندوق خطابات مقدم خدمات الانترنت حتى يقوم المرسل إليه بإدخالها في نظامه المعلوماتي، فهل تعتبر بيانات معلوماتية مخزنة وبالتالي تطبق عليها الإجراءات المتعلقة بالبيانات الساكنة، أم أنها بيانات في مرحلة النقل والتحويل، وبالتالي تطبق عليها الإجراءات المتعلقة بالبيانات المتحركة والمتمثلة في مراقبة (اعتراض) الاتصالات الإلكترونية، وبالتالي لا يجوز الحصول عليها إلا من قبل السلطة المخولة لها ذلك.

حسم المشرع الأمريكي هذا الأمر، واعتبر الاتصالات الالكترونية المخزنة من قبيل البيانات الساكنة، وتطبق عليها كل الإجراءات التي تتناسب مع هذا النوع من البيانات، وقام بتعديل قانون خصوصية الاتصالات الالكترونية ليشمل حماية الاتصالات الالكترونية المخزنة من بريد إلكتروني، ورسائل صوتية غير مفتوحة مخزنة لدى مزود الخدمة.

ميزت اتفاقية بودابست بين البيانات المتعلقة بالمرور والبيانات المتعلقة بمحتوى الاتصال، وعلى العكس من ذلك فإن دولا كفرنسا لم تميز بين تجميع حركة البيانات ومراقبة محتواها، ومن ثم تسري الضمانات ذاتها عند اتخاذ الإجراءين.[1]

الأصل أن مراقبة الاتصالات الالكترونية الخاصة محظور إلا بإذن قضائي مسبق، غير أن هناك حالات تجوز فيها المراقبة دون صدور إذن، حيث تسمح بعض التشريعات كالقانون الأمريكي بوضع أجهزة لتسجيل الاتصالات الإلكترونية في حالة الضرورة إذا توافر خطر حال، وما دام قد توافر

[1] عائشة بن قارة، المرجع السابق، ص167.

من الأسباب ما يدعو إلى الاعتقاد بأن الإذن سوف يصدر، فإذا لم يصدر الإذن بذلك خلال مدة 48 ساعة وجب إنهاء المراقبة فورا.[1]

كما يجوز لمزودي الخدمة مراقبة الاتصالات الالكترونية الخاصة بالمشتركين في إطار المراقبة المعتادة من أجل حماية أنظمتهم من إساءة الاستعمال أو الإضرار بها أو الاستيلاء عليها وقد قررت بعض التشريعات كالقانون الأمريكي هذا الحق، ومن ثم فإن القانون الأمريكي يسمح لمزودي الخدمة بتسجيل التداخلات والتبليغ عنها للضبطية القضائية، غير أنه لا يجوز لرجال الضبط القضائي أن يبادروا إلى المراقبة دون تبليغ من مزودي الخدمة أو حصولهم على إذن مسبق، ومن أمثلة ذلك ما قضي به في قضية تتلخص وقائعها في أن رجال الضبط القضائي كانوا يتتبعون متهما في جريمة اختطاف عمد إلى استعمال خط هاتفي مقلد، مما جعل رجال الضبط القضائي يلجأون إلى مزود خدمات الاتصالات السلكية لمراقبة هذا الخط، لأن القانون يسمح للمزود بتلك الرقابة في حالة وقوع اعتداء على حق من حقوقه، منها سرقة الخطوط، غير أن المحكمة لاحظت أن المبادرة بمراقبة الخطوط يجب أن تبدأ من مزودي الخدمات أثناء قيامهم بأعمالهم، ولهم حينئذ أن يقوموا بتبليغ رجال الضبط، وعكس ذلك غير جائز كما هو الأمر في قضية الحال.[2]

غير أن المشرع الأمريكي لم يطلق سلطة مزودي الخدمات في ممارسة الرقابة، بل حاول الموازنة بين مصالح متعارضة: مصلحة مزود الخدمات، ومصلحة الأشخاص، لذا اشترط جملة من الشروط من الواجب توافرها لصحة المراقبة.[3]

كما تجوز المراقبة دون إذن، بناء على شكوى المشترك في القانون الأمريكي، في حالة الطلب الصادر من صاحب الجهاز محل الاعتداء بوضع جهازه تحت المراقبة من قبل رجال الضبط القضائي وفق شروط معينة.[4]

---

[1] شيماء عبد الغني، المرجع السابق، ص206.

[2] شيماء عبد الغني، المرجع السابق، ص221.

[3] المرجع نفسه، ص223-224.

[4] المرجع نفسه، ص225.

لا تكون المراقبة الالكترونية جائزة كأصل عام إلا بعد الحصول على إذن مسبق مكتوب من السلطة القضائية المختصة حسب ما نصت عليه م3 من القانون 09-04 سالف الذكر والتي حددت أيضا الحالات التي يجوز فيها اللجوء إلى المراقبة الإلكترونية.

الملاحظ أن المشرع الجزائري في م65 مكرر 5 من ق ا ج أجاز لوكيل الجمهورية المتخصص أن يأذن باعتراض المراسلات التي تتم عن طريق وسائل الاتصال السلكية واللاسلكية، إذا تعلق الأمر بجرائم منها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات؛ ويرى البعض أن الأمر يتعلق هنا بالمراسلات العادية التي تتم عبر وسائل الاتصال السلكية اللاسلكية وهي جميع المراسلات أو الرسائل والبرقيات والمحادثات السلكية واللاسلكية المرسلة عن طريق البريد.[1]

الملاحظ أن المشرع الجزائري استخدم في م65 مكرر 5 من ق ا ج وما بعدها مصطلح "اعتراض"، واستعمل في م3 من القانون 09-04 سالف الذكر مصطلح "مراقبة"، للتعبير عن الفعل ذاته، والأولى الثبات على مصطلح واحد.

أجازت م65 مكرر 5 من ق ا ج في فقرتها الثانية وضع الترتيبات التقنية دون موافقة المعنيين من أجل التقاط وتثبيت وبث وتسجيل الكلام المتفوه به من شخص أو عدة أشخاص بصفة خاصة أو سرية سواء أكانت الأمكنة عامة أم خاصة أم سرية، كما أجازت الدخول إلى المحلات السكنية أو غيرها في أي وقت دون علم أو رضا أصحابها، بمعنى أنها أجازت انتهاك بعض الحقوق الشخصية الرئيسة التي نصت عليها القوانين والمواثيق الدولية إذا اقتضت ضرورات التحري في الجرائم المتلبس بها والتحقيق في الجرائم المعلوماتية ذلك، والضمانة هي إذنُ وكيل الجمهورية وممارسة هذه المهام تحت مراقبته المباشرة، وفي حالة فتح تحقيق قضائي، فقاضي التحقيق هو من يصدر الإذن ويراقب العمليات المذكورة.

فرضت م65 مكرر 6 من ق ا ج ضرورة الالتزام بالسر المهني، كما أكدت مبدأ عاما في القانون الجزائي وهو عدم بطلان الإجراءات العارضة، بمعنى أنه إذا اكتشفت جرائم أخرى بطريقة عارضة، غير تلك التي ورد ذكرها في إذن القاضي، فيجوز متابعة مرتكبيها دون أن يمس إجراءات المتابعة على هذه الجرائم البطلان.

[1] زيدان زيبحة، المرجع السابق، ص124.

فرضت م65 مكرر 7 من ق ا ج أن يتضمن الإذن المذكور في م65 مكرر 5 من ق ا ج، جميع العناصر التي تسمح بالتعرف على الاتصالات المطلوب التقاطها، والأماكن المقصودة، والجريمة التي تبرر اللجوء إلى مثل هذه التدابير، ومدتها التي لا تتجاوز أربعة أشهر قابلة للتجديد حسب مقتضيات التحري أو التحقيق.

أجازت م65 مكرر 8 من ق ا ج لوكيل الجمهورية أو ضابط الشرطة القضائية الذي أذن له، ولقاضي التحقيق أو ضابط الشرطة القضائية الذي ينيبه، تسخير الأعوان المؤهلين لدى مصلحة أو هيئة عمومية أو خاصة مكلفة بالمواصلات السلكية واللاسلكية للتكفل بالجوانب التقنية المتعلقة بالاعتراض، كما أجازت م65 مكرر 10 من ق ا ج الاستعانة بمترجم لنسخ وترجمة المكالمات التي تتم باللغات الأجنبية.

بناء على ما تقدم، ترتب المراقبة الصحيحة المتخذة في ظل احترام الضوابط المقررة قانونا أثرا يتعلق بجواز الاعتداد بها كأدلة إلكترونية مقبولة لإثبات الجريمة الإلكترونية الواقعة على التجارة الإلكترونية وغيرها، ونسبتها إلى المتهم، أما المراقبة التي لا تحترم الشروط المقررة في القانون فترتب أثرا عكسيا، يتمثل في استبعاد الأدلة الناجمة عنها، وعدم قبولها في إثبات إدانة المتهم، كونها باطلة، فضلا عن ذلك تتحقق في بعض القوانين المسؤولية الجزائية عن الاعتراض غير المشروع، إذا توافرت الشروط التي يتطلبها القانون لقيام هذه الجريمة (م309 مكرر ق ع م).[1]

[1] عائشة بن قارة، المرجع السابق، ص178.

المبحث الثاني: الحماية الجزائية للتجارة الإلكترونية في مرحلة المحاكمة.

تكفل النصوص العامة بالإضافة إلى النصوص الخاصة في الإجراءات الجزائية حماية قانونية للتجارة الإلكترونية في مرحلة المحاكمة، سواء من حيث تحديد المحكمة المختصة بنظر الجرائم الواقعة على التجارة الإلكترونية (المطلب الأول)، أو من ناحية سلطة المحكمة المختصة في قبول وتقدير الدليل في مجال التجارة الإلكترونية (المطلب الثاني).

المطلب الأول: تحديد المحكمة المختصة في الجرائم الواقعة على التجارة الإلكترونية.

إن قواعد القانون الجنائي – بشقّيه الموضوعي والإجرائي – تخضع في تطبيقها من حيث المكان لمبدأ مستقر ومعروف، ألا وهو مبدأ الإقليمية، الذي يعني خضوع الجرائم التي تقع في إقليم دولة معينة لقانونها الجنائي النافذ، بحيث تصبح محاكمها هي صاحبة الولاية بنظر الدعوى الناشئة عنها، ولا تخضع من حيث الأصل لسلطان أي قانون أجنبي، وفي المقابل لا يمتد سريان قانون الدولة الجنائي خارج نطاقها الإقليمي وفقاً لحدودها المعترف بها في القانون الدولي إلاّ في أحوال استثنائية اقتضتها حماية المصالح الجوهرية للدولة أو متطلبات التعاون الدولي في مكافحة الإجرام، والغالب في الجرائم التقليدية، أن عناصر الركن المادي للجريمة تكتمل في مكان واحد، أو بالأحرى في نطاق إقليم دولة واحدة، حيث يقع السلوك الإجرامي، وتترتب نتيجته الضارة في إقليم دولة واحدة، كأن يقدم أحدهم على طعن المجني عليه أو إطلاق الرصاص عليه، مما يؤدي إلى وفاته في الحال أو بعد لحظة وجيزة، ومن ثم تعتبر الجريمة مرتكبة في هذا المكان، وعلى ضوء ذلك يتحدد القانون الواجب التطبيق، وبالتبعية المحكمة المختصة بنظر الدعوى، بيد أن بعض الجرائم يتجاوز مداها حدود الدولة، حينما يتجزأ ركنها المادي أو يتوزع على أكثر من مكان بحيث يمكن وقوع السلوك في إقليم دولة (س)، في حين تتحقق النتيجة الجرميّة الضارة في نطاق إقليم دولة أخرى (ص)، ومن أمثلة ذلك، أن يطلق شخص النار من داخل الأراضي الليبية تجاه آخر موجود على الأراضي الجزائرية، فيرديه قتيلا أو العكس.

و غالبا ما تثور مشكلة الاختصاص، إذا تعلق الأمر بنوع معين من الجرائم، خاصة الجرائم العابرة للحدود الإقليمية للدول، مثل جرائم تلويث البيئة البحرية والهوائية والاتجار بالمخدرات

وتبييض الأموال والقرصنة المعلوماتية، والجرائم الواقعة على التجارة الإلكترونية وغيرها؛ مما يدفع إلى التساؤل التالي: هل تحقق الركن المادي بالنسبة لهذه الجرائم يكون بمكان وقوع السلوك الإجرامي أم بالمكان الذي تحققت فيه النتيجة؟ [1]

لقد حاول الفقه الإجابة عن هذا التساؤل منذ وقت مبكر، من أجل حل مشكلة تنازع القوانين من حيث المكان، بصدد هذه الفروض المثارة، وانقسم إلى ثلاثة اتجاهات (الفرع الأول)، وحسمت بعض التشريعات الوطنية الخلاف من خلال تدخل تشريعي بيّن القانون الواجب التطبيق والمحكمة المختصة في مثل هذه الحالات (الفرع الثاني).

الفرع الأول: الموقف الفقهي من تنازع الاختصاص الجنائي.

ذهب الاتجاه الأول من الفقه إلى أن العبرة في تحديد مكان وقوع الجريمة بالمكان الذي وقع فيه السلوك بقطع النظر عن المكان الذي تحققت فيه النتيجة، أو من المفترض تحققها فيه، وفي المقابل ذهب اتجاه آخر إلى أن مكان وقوع الجريمة يتحدد بالمكان الذي تحققت فيه النتيجة أو كان من المفترض تحققها فيه، وبين هذا وذاك رأى اتجاه ثالث إلى أن العبرة في ذلك تكون بمكان حصول أي منهما (السلوك أو النتيجة)، ولكل مذهب من هذه المذاهب مبرراته وأسانيده التي تعززه وتدعمه، علما أن هذه الآراء لا تخص الجرائم الإلكترونية وحدها.

أولا : مذهب السلوك أو النشاط الإجرامي بوصفه معيارا لتحديد مكان وقوع الجريمة.

وفقا لهذا المعيار، ينعقد الاختصاص للمحكمة التي يقع في نطاقها النشاط الإجرامي، وليس مكان حصول النتيجة أو الآثار المترتبة عليه، بدعوى أن اتخاذ آثار الفعل كمناط لتحديد مكان وقوع الجريمة تكتنفه بعض الصعوبات؛ يمكن إجمالها في أنه معيار مرن وفضفاض، فضلا عن أن معيار حصول النشاط أدعى إلى تيسير عملية الإثبات وجمع أدلة الجريمة، وأن المحكمة التي لها ولاية نظر الدعوى تكون قريبة من مسرح الجريمة، ناهيك عن أن الحكم الذي يصدر في الواقعة يكون أكثر فعالية ويسهل معه ملاحقة الجناة.

---

[1] أ د موسى مسعود أرحومة، الإشكاليات الإجرائية التي تثيرها الجريمة المعلوماتية، بحث مقدم إلى المؤتمر المغاربي الأول حول المعلوماتية والقانون، طرابلس ليبيا 2009، ص15. (منشور على الانترنت).

ويضيف المؤيدون لهذا الاتجاه حججاً أخرى، منها أن حدوث الضرر في مكان معين مردّه في الغالب إلى أسباب لا إرادة لمقترف السلوك فيها، وأن من شأن تطبيق قانون الدولة التي تحقق في نطاقها الضرر لا يتفق واعتبارات العدالة نظراً لجهل الجاني بهذا القانون الذي يتم إعماله بحقه، وفي الغالب ليس ممكنا العلم به؛ إذ حينما أقدم على ارتكاب الفعل الذي أتاه يعتقد مشروعيته وفقاً لقانون البلد الذي وقع فيه السلوك، وإذا به غير ذلك من منظور قانون البلد الذي تحقق فيه الضرر.

وقد حظي هذا الاتجاه بتأييد جانب كبير من الفقه سواء في فرنسا أو مصر، ليس هذا فحسب، بل اتجهت بعض التشريعات المقارنة إلى تبنيه، ومن هذا القبيل القانون النمساوي الصادر سنة 1979 والمجري الصادر في السنة ذاتها.[1]

ثانيا : مذهب مكان تحقق النتيجة كمعيار لتحديد الاختصاص.

على الرغم من الحجج التي ساقها مؤيدو المذهب الأول، فإن هذا الاتجاه تعرض لجملة من الانتقادات من جانب آخر من الفقه، وقد انصبّت هذه الانتقادات على أن هذا المذهب لا يعير اهتماماً للمكان الذي تحقق فيه الضرر أو أثر النشاط الإجرامي الذي كان الجاني يسعى إلى تحقيقه فيه؛ فالآثار الضارة هي التي تبعث الفزع في نفوس الناس، في حين أن مكان وقوع السلوك لا يعدو أن يكون مصدر الضرر ليس إلاّ، كما أن تمام الجريمة لا يكون إلاّ في المكان الذي ظهرت فيه آثارها الضارة التي كان الجاني يقصدها أو يرغب في تحقيقها.

يضاف إلى ذلك أن تقادم الجريمة يتم احتسابه من الوقت الذي تحققت فيه النتيجة، كما يؤخذ في الحسبان جسامة الضرر كأساس لتقدير التعويض ولا عبرة بخطورة الفعل أو درجة الخطأ، كذلك يعد حصول الضرر شرطاً أساسياً لقيام المسؤولية المدنية، فتنفى هذه المسؤولية متى ما انتفى الضرر، ومن ثَم لا مصلحة للمدعي في الدعوى، ما يجعلها بالتالي غير مقبولة.

ومن المبررات التي سيقت لتعزيز هذا الاتجاه أن الأخذ به يحقق وحدة الجريمة وعدم الفصل بين عناصرها، كذلك يمتاز هذا الاتجاه في نظر المدافعين عنه بأنه أكثر واقعية على اعتبار أن

[1] موسى مسعود أرحومة، المرجع السابق، ص16.

الضرر له مظهر خارجي ملموس خلافا للنشاط الذي قد لا يكون كذلك متى ما اتخذ صورة الامتناع أو السلوك السلبي.

ومن هنا، فقد لقي هذا الاتجاه ترحيباً من بعض الفقه إلى جانب ذلك تم تبنيه من بعض التشريعات المقارنة، ومنها القانون الألماني الصادر سنة 1975، والقانون الدولي الخاص التركي الصادر سنة 1982، كما أقرّته اتفاقية بروكسل لسنة 1969 بشأن المسؤولية عن أضرار التلوث بالبترول.

بالإضافة إلى ذلك دأب القضاء على تطبيقه في بعض المناسبات، من ذلك في واقعة عرضت على القضاء الأمريكي مؤداها أن قام رئيس فرقة، وهو على متن مركب أمريكي على قتل شخص موجود بمركب أجنبي بإطلاق النار عليه، وعند تقديمه للقضاء قضى بعدم اختصاصه بهذا الفعل مؤسساً ذلك على أن الوفاة (النتيجة) قد تحققت على متن مركب أجنبي.

ومع ذلك، فإن هذا الاتجاه لم يكن بمنأى هو الآخر عن النقد، الذي يتركز في أن الأخذ به يفضي في نهاية المطاف إلى عدم تجريم الشروع إذا لم تتحقق النتيجة، وكذلك عدم العقاب على ما يُعرف بالسلوك المجرد (جرائم السلوك المجرد).

ثالثا: المذهب المختلط.

أمام الانتقادات التي تعرض لها كلا من الاتجاهين السابقين، برز اتجاه ثالث مفاده أن الجريمة تعد واقعة في مكان حصول النشاط (العمل التنفيذي)، وكذلك المكان الذي تحققت فيه النتيجة أو الذي من المتوقع أو من المنتظر تحققها فيه، وهذا الاتجاه حظي بمباركة أغلب الفقه، ويجد مبرره في أن الركن المادي للجريمة يقوم على ثلاثة عناصر، وهي الفعل (النشاط)، والنتيجة، وعلاقة السببية، ما يعني أن الجريمة تعد واقعة في كل مكان تحقق فيه عنصر من عناصر الركن المادي، أي في مكان النشاط ومكان النتيجة على حد سواء.

وهذا الاتجاه أخذت به بعض التشريعات المقارنة، كما تبنته المحاكم في بعض الدول ومنها فرنسا في عدد من الأحكام، إذ ذهبت إلى أن اختصاصها يتسع ليشمل كل الأمكنة التي كانت مسرحاً للجريمة عند وقوعها.

وقد قضي بأن المحكمة تعتبر مختصة بالدعوى الناشئة عن جريمة إصدار صك دون مقابل الوفاء فيما يخص صكاً كان محرراً خارج فرنسا ومسحوباً على أحد البنوك فيها.[1]

وتكرر ذلك في واقعة أخرى عرضت على القضاء المذكور يقر فيها باختصاصه بصدد جريمة نصب متى ارتُكِبت أفعال النصب (الطرق الاحتيالية) أو تسليم النقود على الإقليم الفرنسي.

ويتم تغليب قانون محل تحقق النتيجة إذا كانت الجريمة تامة، ومن قبيل ذلك جرائم السلوك والنتيجة (الجرائم المادية)، في حين يفضل مكان النشاط أو السلوك إذا كانت الجريمة قد وقفت عند حد الشروع أو كانت من قبيل جرائم السلوك المجرد.

وبالوقوف على المبررات التي استند إليها كل اتجاه مما تقدم وما يكتنفه من قصور، يرى كثير من الفقه أن الاتجاه الأخير يَفضُل ما عداه، لكونه تجاوز المآخذ التي اعترت المذهبين الآخرين، وفي الوقت ذاته استجمع ميزات كل منهما؛ فهو يوسع من نطاق الحماية الجزائية ويتيح مرونة أكثر في مد نطاق الاختصاص، لاسيما وأن بعض الأفعال مجرَّمة في ذاتها، ولا ينجم عنها أي ضرر مادي، ومنها ما تمتد آثاره الضارة لدولة أو دول أخرى غير التي وقع فيها النشاط، الأمر الذي يهدد مصالحها الحيوية. وربما يكون أكثر انسجاما مع الطبيعة المميزة لجرائم الإنترنت والتجارة الإلكترونية على وجه الخصوص وبما يكفل حل مشكلة تنازع الاختصاص الناجمة عنها.

الفرع الثاني: الموقف التشريعي والقضائي من تنازع الاختصاص الجزائي الدولي.

للتغلب على مشكلة الاختصاص الجزائي الدولي التي تثيرها بعض الجرائم، ومنها تلك الواقعة على التجارة الإلكترونية، عمدت الكثير من التشريعات المقارنة إلى وضع قواعد قانونية يتم بمقتضاها تحديد المحكمة المختصة والقانون الواجب التطبيق، وقد حثت بعض الاتفاقيات الأطراف المتعاقدة على تبني هذا النهج، من ذلك الاتفاقية العربية لمكافحة جرائم تقنية المعلومات في م30 منها، وهو ما نصت عليه قبل ذلك اتفاقية بودابست لسنة 2001 في المادة 22، كما أثارت م15 من القانون 09-04 سالف الذكر مشكلة الاختصاص القضائي.

[1] موسى مسعود أرحومة، المرجع السابق، ص18.

لا تخرج المواقف التشريعية للدول عن أربعة مبادئ هي: مبدأ الإقليمية، مبدأ العينية، مبدأ الشخصية، ومبدأ عالمية الاختصاص.

أولا: مبدأ إقليمية النص الجزائي.

يعني مبدأ الإقليمية، أن الإقليم الخاضع لسيادة الدولة بحدوده المعرفة هو الذي يحدد نطاق تطبيق النصوص الجزائية الوطنية، سواء الموضوعية أو الإجرائية، فالتشريع الجزائي للدولة يطبق على كافة الجرائم المرتكبة داخل إقليمها بغض النظر عن جنسية مرتكبيها، ولمبدأ الإقليمية مبررات عديدة منها أن القانون الجزائي هو أداة الدولة في فرض سلطان سيادتها على إقليمها، وأن الحفاظ على مصالح وحقوق أفراد المجتمع مظهر من مظاهر تلك السادة، كما أن المكان الذي تقترف فيه الجريمة يعد أنسب الأمكنة لمحاكمة المتهم لاعتبارات عديدة،[1] ولهذا المبدأ نتيجتان: إيجابية وسلبية، فالإيجابية تتمثل في أن أحكام تشريع الدولة تطبق على جميع الجرائم التي تقع في إقليمها سواء أحمل جنسيتها أم كان من الأجانب طالما أنه متواجد على إقليمها، فالعبرة بمكان وقوع الجريمة، كذلك أدرجت بعض التشريعات ضمن هذا المبدأ من كان خارج إقليم الدولة، ولكنه أتى فعلا جعله فاعلا أو شريكا في الجريمة الواقعة على إقليم الدولة، من هذه التشريعات ما نصت عليه م1/2 ق ع م؛ أما النتيجة السلبية فتتمثل في عدم تطبيق نصوص القانون الجزائي الوطني على أي شخص يرتكب جريمة كاملة خارج الإقليم، ولا عبرة هنا بصفة الفاعل في ارتكاب الجريمة إعمالا لفكرة السيادة.

نصت م1/3 من ق ع على أن قانون العقوبات يطبق على كافة الجرائم التي ترتكب في أراضي الجمهورية، ونص المشرع الفرنسي على الأمر نفسه في م 2/113 ق ع ف، وأوضحت بأن الجريمة تعد مرتكبة على إقليم فرنسا إذا ارتكب أحد عناصر الجريمة على إقليمها، وحددت م1/113 المقصود بالإقليم الفرنسي، كما أن م5/113 ق ع ف نصت على:"يطبق قانون العقوبات الفرنسي على كل من يرتكب فعلا في إقليم الجمهورية يجعله شريكا في جناية أو جنحة ارتكبت في الخارج إذا كان معاقبا عليها في القانون الفرنسي والقانون الأجنبي، وكانت ثابتة بموجب حكم نهائي من القضاء الأجنبي"، المعنى ذاته نص عليه المشرع الجزائري في م585 ق ا ج، كما نصت م586 ق ا ج على: "تعد مرتكبة في الإقليم الجزائري كل جريمة يكون عمل من الأعمال المميزة لأحد أركانها قد تم في

[1] باسم شهاب، مبادئ القسم العام لقانون العقوبات، د م ج، وهران، الجزائر 2007، ص35.

الجزائر"، ونصت م15 من القانون 09-04 سالف الذكر على: "...تختص المحاكم الجزائية بالنظر في الجرائم المتصلة بتكنولوجيا الإعلام والاتصال المرتكبة خارج الإقليم الوطني، عندما يكون مرتكبها أجنبيا وتستهدف مؤسسات الدولة الجزائرية أو الدفاع الوطني أو المصالح الإستراتيجية للاقتصاد الوطني" ووفقا لذلك فإنه لتحقق الجريمة داخل إقليم الدولة في فرنسا أو مصر أو الجزائر، يجب أن يتخذ من إقليم الدولة مكانا لأي من عناصر السلوك، أو النتيجة، فأيا منهما يكون كافيا لانعقاد الاختصاص المكاني للنص الجزائي على الواقعة، ويجد هذا الأمر صداه في التشريعات المقارنة في نطاق الجرائم الإلكترونية، فالو م أ تعطي الاختصاص لمحاكمها الجزائية إذا حدثت آثار الجريمة على إقليمها، وهو ما يعرف بمبدأ النتيجة الإجرامية الذي يسمح للدولة بمتابعة المتهم لقاء ما حاق بها من ضرر، وأول تطبيق للمبدأ المذكور كان في قضية عرفت ب"آل توماس"[1] سنة 1991،[2] وطبق المبدأ ذاته في

---

[1] طارق فوزي، المرجع السابق، ص237.

[2] في عام 1991 قام زوجان أمريكان من مدينة "ميلبيتاس" بولاية كاليفورنيا بنشر مواد دعارة عبر الانترنت مع السماح للغير بالولوج إلى نظام النشر الحاسوبي "BBS" خاص بهم حيث تضمن نظام "BBS" حوالي(14.000) صورة داعرة بنظام ملفات "GIF" ومراسلات داعرة وطلبات لشرائط فيديو، وبعد عدة محاولات فاشلة لإدانة مشغلي نظام"BBS" المذكورة في مدينة"بركلي" بولاية كاليفورنيا، قام رجال مباحث الخدمات السرية بإنزال الملفات الفاحشة المذكورة في حاسوب متواجد في ولاية"تينسي" ومن ثم أمكن تقديمهم هناك للمحاكمة وفقا لمبدأ حدوث النتيجة الإجرامية.

قضاء أول درجة:

قضت محكمة أول درجة في 1994/12/2 بعقابهما بالحبس سبعة وثلاثين شهرا، وهو ما دعاهما لإقامة استئناف في 1994/12/9 وكان من أوجه الاستئناف أنهما لم يقوما بإحداث عملية إنزال للملفات "GIF" التي تحوي صورا فاضحة في ولاية (تينسي)، وإنما الذي قام بذلك ودون علمهما هو العميل الخاص بمراقبة البريد الفيدرالي، ومن ثم فإن نشاطهما المادي لا يمتد إلى ولاية (تينسي) وإنما انحصر في ولاية (كاليفورنيا) مما يعني عدم اختصاص قضاء ولاية "تينسي" بنظر هذه القضية.

حكم محكمة الاستئناف

رفضت محكمة الاستئناف الدفاع المقدم من الزوجين استنادا إلى النصوص القانونية التي تحكم هذه الواقعة، فهي فضلا عن كونها نصوصا فيدرالية تختص كافة المحاكم الأمريكية بتطبيقها دون تقرير خاص بذلك، فهي أيضا تتضمن جرائم ذات طبيعة مستمرة، واعتبرت المحكمة الاستئنافية أن مسرح الجريمة هو كل مكان يمتد إليه البث عبر الانترنت وهو هنا ولاية (تينيسي).

كما أقرت محكمة أمريكية بأن النائب العام (لمينيسوتا) لديه اختصاص للادعاء في (مينيسوتا) على المدعى عليه (نيفادا) الذي يدير موقعا للمقامرة، كأحد النشاطات الإجرامية المدارة عبر الانترنت.

وهنا قدم النائب العام (لمينيسوتا) دعوى حماية للمستهلك للادعاء على ممارسات الغش في التجارة، الإعلان الكاذب، والاحتيال على المستهلك. المدعى عليه أدار موقعا للمراهنة الرياضية والتي تقدم (بشكل غير صحيح)، أن الرهان عبر خدمتها على الانترنت قانوني. المدعى عليه يتفاخر في إعلاناته بأن إعلاناته رائجة عبر البلاد، وستصل إلى مليوني مستهلك. وقائمة بريد المدعى عليه تشمل مقيمين (مينيسوتا). وخلال مدة أسبوعين، دخل (248) مقيم في (مينيسوتا) للموقع على الأقل. المدعى عليه تابع التعقب للدخول إلى الموقع وهو يعلم أن العديد من الزبائن من (مينيسوتا). وقد حذر الموقع الزبائن من أن المدعى عليه له الحق في أن يقاضيهم جميعا، إما في دولتهم أو في (مينيسوتا)، في أي نزاع يتعلق بحسابات رهانهم.

كان يدار الموقع المذكور حقيقة من قبل شركة أخرى، لم تكن طرفا مدعى عليه في القضية أي أنها كانت شركة أجنبية خارج الولايات المتحدة وهذا لن يغير تحليل المحكمة المتعلق بتوفر الاختصاص.

فرنسا في قضية رفعتها رابطة الطلبة اليهود ضد شركة Yahoo، وعرفت ب: " LICRA et UEJF"[1]، كما أكدت المحاكم الفرنسية أن القاضي الجزائي الفرنسي مختص بالنسبة لنص بُث عبر الانترنت من الخارج، إذا كان بالإمكان أن يستقبل في فرنسا.[1]

كما قضى في الولايات المتحدة الأمريكية في قضية ثالثة باختصاص محكمة ولاية "كونكتيكوت" بنظر دعوى بخصوص دعاية كاذبة استنادا إلى أن البث عبر الانترنت كان يستطيل إلى تلك الولاية.

وقضى أيضا بالولايات المتحدة الأمريكية في قضية رابعة باختصاص محكمة ولاية "ميسوري" بالنظر في قضية تقليد علامة تجارية. رغم أن المتهم في هذه القضية كان يقيم بولاية كاليفورنيا استنادا إلى أن الموقع الذي يبث منه المتهم العلامة التجارية المقلدة يقع في ولاية "ميسوري" وأنه يكفي أن يستطيل البث إلى ولاية "ميسوري" حتى ينعقد الاختصاص لمحاكمها بنظر الدعوى. سامح أحمد، المرجع السابق، ص406-407.

قضت محكمة في ميونخ في حكمها الصادر في 1998/5/28 بمسؤولية "computer server ger" وهي فرع كامل للشركة الأم في الولايات المتحدة الأمريكية عن وجود مواقع دعارة حتى، ولو كان مزود الاستضافة لهذه المواقع هو المركز الرئيس في الولايات المتحدة الأمريكية، وقررت المحكمة أنه يجب اعتبار الفرع في ألمانيا مزود استضافة لكونه ذا علاقة وطيدة بالمزود في الولايات المتحدة، إذ أن المركز الرئيس يعد طريق بث إلى الخوادم الأخرى التابعة له عبر العالم.

وقد جاء هذا الحكم تطبيقا لقانون الوسائط المتعددة الألماني لسنة 1997 والذي بمقتضاه ينعقد الاختصاص للقضاء الألماني إذ كان البث يصل إلى الأراضي الألمانية. المرجع السابق، ص407.

وفي إيطاليا: المدعى عليها في هذه الدعوى مؤسسة إيطالية، وكان المدعي قد تعرض لإصابة عندما كان نزيلا في أحد فنادق المدعى عليه في ايطاليا، المدعى عليها لم تمارس أي عمل في نيوجيرسي. لكنها تقوم بعرض صور لغرف الفندق وشروحات لمرافق الفندق ومعلومات عن عدد الغرف وأرقام الهواتف على الانترنت.

المحكمة وافقت على أن إعلانات كهذه على الانترنت تقع ضمن طريقة الإعلان، كإعلان في مجلة وطنية ولا تشكل"اتصالا مستمرا وجوهريا" مع دولة النطاق المكاني، ولهذا قررت المحكمة أن الإعلان على الانترنت ليس معادلا في توجيه النشاط إلى انتهاز الفرصة بشكل مستهدف في نطاق مكاني خاص.

وهنا يتم التطرق إلى مسألة مدى انطباق قانون دولة ما، يكون مزود خدمة الانترنت الموجود بإقليمها مجرد فرع تابع لمركز رئيسي في دولة أخرى في حالة بث مواد تشكل سلوكا إجراميا وفقا لقانون دولة الفرع. وتقاربت التشريعات المقارنة في تقرير الاختصاص القضائي لمحاكمها ما دامت الواقعة الإجرامية تمتد إلى إقليم الدولة.المرجع السابق ص407.

[1] المرجع نفسه، ص 238، يراجع أيضا الغافري، المرجع السابق، ص581، وأيضا: سامح أحمد، المرجع السابق، ص404.

في دعوى قضائية معروفة في القضاء الفرنسي رفعت من رابطة الطلبة اليهود التي تحارب العنصرية ومناهضة السامية وتسمى LICRA ET UEGF ضد شركتي YAHOO INC ET YAHOO FRANCE وقد طالب فيها المدعى أمام رئيس محكمة باريس الابتدائية (قضاء مستعجل) بالحكم بمنع هاتين الشركتين من السماح لمستخدمي الانترنت الفرنسيين بالدخول على منافذ المواقع التي يعرض عليها نظام البيع بالمزاد العلني للأشياء المتحصلة من النازية، وقد أثارت هذه الدعوى نزاعا بين القانون الفرنسي الأمريكي، وهو ما حسمه رئيس المحكمة في قراراته الصادرة في تاريخ 22 مايو، 11 أوت، 2 نوفمبر سنة 2000 ، مقررا اختصاص القانون الفرنسي بحل هذا النزاع على أساس احترام القانون الفرنسي.

إن هذه الأشياء ظاهرة للعيان في فرنسا وأنه بممارسة مستخدمي الانترنت في فرنسا لمثل هذا النوع من البيوع يرتكبون خطأ على الإقليم الفرنسي، فضلا عن أن الضرر قد وقع في فرنسا، وبذلك يصبح القضاء الفرنسي هو المختص بالنزاع طبقا للمادة(2/46) من قانون الإجراءات الجنائية الفرنسي والمادة (113-2) من قانون العقوبات الفرنسي.

وبذلك يكون رئيس المحكمة قد اعتمد على مكان حدوث الفعل الضار والنتيجة الإجرامية، وإن كانت"ياهوو فرنسا" فرعا للمركز الرئيس بالولايات المتحدة الأمريكية، إلا أن البث يصل إلى الإقليم الفرنسي .

ثانيا: مبدأ شخصية النص الجزائي.

يعني شخصية النص الجزائي أن يطبق على كل من يحمل جنسية الدولة بغض الطرف عن مكان وقوع الجريمة، والمصالح المحمية التي انتهكت نتيجة وقوع الجريمة، فالاعتبار هنا لمرتكب الجريمة (والضحية بالنسبة للقانون الفرنسي) لا مكان ارتكابها، وميز المشرع بدوره بين الجناية والجنحة واستبعد المخالفة، والعبرة بوقت ارتكاب الجريمة ولو فقد مرتكبها جنسيته بعد ذلك.[2]

مبدأ شخصية النصوص الجزائية له وجهان أحدهما إيجابي يعني تطبيق النص الجزائي على كل من يحمل جنسية الدولة، والوجه الآخر سلبي، ويعني تطبيق النص الجزائي على كل جريمة تكون الضحية فيها تتمتع بجنسية الدولة، ولم ينص كلا من المشرع الجزائري والمشرع المصري إلا على الوجه الإيجابي للمبدأ،[3] على خلاف المشرع الفرنسي الذي نص على الوجهين في قانون العقوبات الفرنسي (م113-6)، ويرى البعض أن مسلك المشرع الفرنسي غير محمود، ومنتقد لما ينطوي عليه من الأنانية وعدم الثقة في قضاء الدولة التي وقعت الجريمة على إقليمها.[4] غير أن هذا المنحى يدل على رغبة قوية في حماية المواطن الفرنسي من الاعتداءات التي قد تلحق به، خاصة إذا كان الفعل غير مجرم في الدولة التي تم من خلالها الاعتداء على الفرنسي.

وقد تبنى القضاء الأمريكي المنحى نفسه الذي أقره المشرع الفرنسي، فقد قضت المحكمة العليا لولاية "نيويورك" بتطبيق مبدأ الاختصاص الشخصي في جريمة انتهاك قانون المستهلك والإعلان الخادع حول مبيعات مجلات عبر البريد الإلكتروني.[5]

يطبق مبدأ شخصية النص الجزائي حتى لو كان المتهم قد اكتسب جنسية الدولة بعد ارتكاب الفعل المنسوب إليه (م584 ق ا ج)، فالمهم هو وضعيته يوم بدء المتابعة القضائية.[1]

ومفاد ذلك كي ينعقد الاختصاص للقضاء الفرنسي فإنه يجب توافر شرطين: الأول هو أن يكون المكان الذي تم منه البث معروفا ومحددا والثاني: أن يكون الفعل الأصلي مجرما قانونا في الخارج، وهذا الشرط إنما يتحدد بتحديد مكان البث لمعرفة ما إذا كان الفعل مجرما أم لا. وهنا يثار التساؤل حول علاقة الأصل بالفرع في موضوع مزود الانترنت وأثر ذلك على الاختصاص القضائي. سامح أحمد، المرجع السابق، ص404.

[1] T. corr. Paris 1998, voir: Jean Larguier et autres, op cit, p239

[2] باسم شهاب، المرجع السابق، ص39.

[3] بموجب التعديل الأخير لقانون الإجراءات الجزائية بالأمر 15-02 سالف الذكر فإن المشرع الجزائري أخذ بالوجه السلبي أيضا لمبدأ شخصية النص الجزائي، عندما أضاف لنص م588 ق ا ج عبارة "...أو جناية أو جنحة ترتكب إضرارا بمواطن جزائري".

[4] د.أحسن بوسقيعة، الوجيز في القانون الجزائي العام، ط4، دار هومة، الجزائر 2006، ص92.

[5] سامح أحمد، المرجع السابق، ص410.

في مجال الجرائم الإلكترونية فإن تطبيق مبدأ شخصية النص الجزائي يصطدم بعقبات كثيرة من أهمها أن محاكمة المتهم المقيم في دولة أجنبية أمر يحتاج إلى إجراءات طويلة وكلفة باهظة، وتشمل المحاكمة هنا جميع إجراءات الضبط والقبض والتحقيق والتقديم للمحاكمة، وتنفيذ الأحكام الأجنبية؛ ومنها أيضا أن عدد الدول الموقعة على اتفاقية تسليم المجرمين يعد قليلا جدا بالمقارنة بعدد الدول التي تنتشر فيها الانترنت انتشارا واسعا؛ ومنها أن المتضرر من الجريمة في الفرض الذي لا يكون فيه القانون الوطني يجرم الفعل الذي أحدث الضرر، يتكبد عناء السفر إلى دولة مرتكب هذا الفعل الذي ألحق الضرر لإقامة دعواه هناك.[2]

ثالثا: مبدأ عينية النصوص الجزائية.

يعني مبدأ عينية النصوص الجزائية تطبيقها على كل الجرائم التي تمس كيان الدولة أو مصالحها الأساسية أيا كان مكان وجنسية مرتكبيها، وعادة لا يتم اللجوء إلى هذا المبدأ كمعيار لتحديد نطاق اختصاص النص الجزائي وانطباقه على الوقائع، ولكن التشريعات تستعين بهذا المبدأ لتكملة مبدأ الإقليمية أو مبدأ الشخصية، أو لمنح النص الجزائي مجالا واسعا قد لا يسمح به أحد هذين المبدأين أو كلاهما.[3]

قد أخذت الجزائر بهذا المبدأ، إذ نصت عليه م588 ق ا ج بأحد شرطين: إما إلقاء القبض على المتهم بالجزائر أو أن يتم تسليمه للحكومة الجزائرية وفق إجراءات التسليم، كما أكدت م15 من القانون رقم 09-04 سالف الذكر هذا المبدأ في مجال الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، وكذلك فعل كل من المشرع الفرنسي (م113-10 ق ع ف) والمشرع الأمريكي، بل غالبية التشريعات المقارنة.

اشترط المشرع الجزائري أن تكون الجرائم مرتكبة من قبل أجنبي، لأن الجزائري يخضع لمبدأ الشخصية، وأن ترتكب خارج إقليم الجزائر لألا تخضع لمبدأ الإقليمية، وأن تمس المصالح الأساسية للجزائر، وهذا وصف واسع يجوز أن يضم تحته جملة من الجرائم،[4] وعليه، لو كانت الجرائم المرتكبة

---

[1] Jacques Leroy, op cit, p152.

[2] سامح أحمد، المرجع السابق، ص412.

[3] سامح أحمد، المرجع السابق، ص413.

[4] باسم شهاب، المرجع السابق، ص42.

على التجارة الإلكترونية من الجسامة بحيث تؤثر على الاقتصاد الوطني أو تمس بالمصالح العليا للوطن، جاز إعمال هذا المبدأ.

أما عن المفاضلة بين كل من مبدأ العينية ومبدأ الإقليمية، فيرى البعض أن الأولوية تكون لمبدأ العينية وحجتهم في ذلك نص م699 ق ا ج.[1]

رابعا: مبدأ الاختصاص العالمي.

يقصد بالمبدأ أن يكون لكل دولة ولاية القضاء على أية جريمة بغض النظر عن مكان وقوعها أو مساسها بمصالحها العليا، أو جنسية مرتكبيها أو المجني عليه فيها، وهو بهذا صعب التطبيق لاعتبارين اثنين أولهما عدم قدرة كافة الدول على هذا الأمر من الناحية العملية، فالقضاء في كثير من الدول يعاني مشاكل كبيرة منها كثرة القضايا المطروحة عليه، وليس من الحكمة أن يتحمل أعباء أخرى تضاف عليه، والثاني أن هذا المبدأ يتطلب أن يكون القاضي ملما بكل القوانين، وهو أمر صعب المنال.[2]

من التشريعات التي تبنت مبدأ العالمية، قانون العقوبات العراقي رقم 111 لسنة 1969 في م13 منه.[3]

تعتبر المحاكم البلجيكية سباقة في مجال الاختصاص العالمي، حيث أصدرت محكمة استئناف بروكسل حكما سنة 2002 قضت فيه برفض الشكوى المقدمة ضد "شارون" على أساس أن المتابعة القضائية لا تجوز ضد شخص غير متواجد على التراب البلجيكي، وقد ألغت محكمة النقض البلجيكية هذا الحكم في 2003/02/12 معتبرة أن شرط وجود المتهم على التراب البلجيكي غير ضروري.[4] وصادق البرلمان بعدها على قانون جديد يعدل قانون 1993، كرس الاختصاص العالمي للمحاكم البلجيكية.[5]

---

[1] المرجع نفسه، ص43.

[2] أحسن بوسقيعة، المرجع السابق، ص93.

[3] باسم شهاب، المرجع السابق، ص42.

[4] أحسن بوسقيعة، المرجع السابق، هامش ص93.

[5] المرجع نفسه، ص94.

جاء حول تبرير فكرة عالمية العقاب أنها تخفف من حدة مبدأ الإقليمية الذي تعتمده التشريعات الجزائية، فمبدأ العالمية لا يقوم على حق سيادة الدولة التي تحاكم المتهم، وإنما على وجوب منع الضرر الذي ينجم عن إفلات الفاعل من المساءلة الجزائية؛ ويقتضي تطبيق هذا المبدأ من الناحية العملية توافر ثلاثة شروط طبقا للعرف الدولي، وهي أن تكون الجريمة المرتكبة من الجرائم عبر الوطنية أي من الجرائم العالمية أو من الجرائم الدولية، مما يجعل دولة ضبط المتهم وكأنها نائبة عن المجتمع الدولي في الملاحقة والعقاب، وكأن دور الدولة في المجتمع الدولي كدور النيابة العامة في المجتمعات الوطنية؛ كما يشترط أن يتم إلقاء القبض على المتهم في إقليم الدولة، وإن كان يجوز محاكمته غيابيا أمام قضاء الدول التي تأخذ بالاختصاص العالمي، والهدف من ذلك هو منع الفاعل من السفر إلى هذه الدولة أو الدول التي تربطها بها اتفاقيات تسليم المجرمين، خشية القبض عليه، أما الشرط الثالث فهو ألا يوجد طلب بتسليم الفاعل من قبل دولة أخرى وفقا لمبدأ الإقليمية أو مبدأ الشخصية، لأن مبدأ العالمية مرجوح أمام هذين المبدأين،[1] فالهدف منه حدوث تكامل قضائي وليس حدوث تنازع اختصاص.

لم يتبن المشرع الجزائري مبدأ العالمية رغم أهميته، ويرى البعض أن المبدأ المذكور يغني عنه النصوص الدولية المصادق عليها، وهو قول صحيح، ولكن لا ضرر من أن ينص عليه أيضا في القانون الجزائي الداخلي.[2]

بخصوص الجرائم الإلكترونية عامة، والجرائم الواقعة على التجارة الإلكترونية بصفة خاصة فهي جرائم عالمية، لا تعترف بالحدود الإقليمية، مما يدعو إلى القول بملاءمة مبدأ العالمية لهذا النوع المستحدث من الجرائم.

[1] فطيمة بوعناد، المرجع السابق، ص 242.

[2] باسم شهاب، المرجع السابق، ص43.

الفرع الثالث: الاختصاص الجزائي الداخلي بالنسبة لجرائم التجارة الإلكترونية

نص المشرع على أنواع اختصاص المحاكم الجزائية، وهي الاختصاص النوعي، الاختصاص بالنسبة لشخص المتهم، والاختصاص المكاني،[1] وبالنسبة للجرائم الواقعة على التجارة الإلكترونية، فإن القواعد العامة المتعلقة بالاختصاص النوعي، والاختصاص بالنسبة لشخص المتهم تطبق عليها دون خصوصية تذكر، أما فيما يتعلق بالاختصاص المكاني فإنه يتحدد حسب القواعد العامة بمكان ارتكاب الجريمة أو مكان إقامة المتهم أو مكان القبض عليه (م329 ق ا ج)، كما ينعقد بمكان إقامة المستفيد من الشيك ومكان الوفاء بالنسبة لجنحتي إصدار شيك دون رصيد، وإصدار شيك رغم منع الشخص من ذلك.[2]

أما الخصوصية بالنسبة للجرائم الماسة ب: STAD، فتتمثل في قيام المشرع الجزائري بعد التعديل الذي أجراه على المواد 37، 40، و329 ق ا ج بموجب القانون 04-14 المؤرخ في 10 نوفمبر 2004،[3] بتمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق، حيث كان التمديد كالآتي: تمديد الاختصاص المحلي لمحكمة سيدي محمد ووكيل الجمهورية وقاضي التحقيق بها إلى محاكم المجالس القضائية للجزائر والشلف والأغواط...(محاكم المجالس القضائية للوسط)، تمديد الاختصاص المحلي لمحكمة قسنطينة ووكيل الجمهورية وقاضي التحقيق بها إلى محاكم المجالس القضائية لقسنطينة وأم البواقي وباتنة...(محاكم المجالس القضائية لشرق البلاد)، تمديد الاختصاص المحلي لمحكمة وهران ووكيل الجمهورية وقاضي التحقيق بها إلى محاكم المجالس القضائية لوهران وبشار وتلمسان...(محاكم المجالس القضائية لغرب البلاد)، تمديد الاختصاص المحلي لمحكمة ورقلة ووكيل الجمهورية وقاضي التحقيق بها إلى محاكم المجالس القضائية لورقلة وأدرار وتمنراست ...(محاكم المجالس القضائية لجنوب البلاد).

ولكن الطبيعة الخاصة للجرائم المعلوماتية وخاصة ما تعلق ببعدها المكاني، والمقصود به وجود الجهاز الذي يتم ارتكاب الجريمة عن طريقه في مكان مختلف، عن المكان الذي يتواجد فيه الجهاز الخادم، جعلت التساؤل التالي يفرض نفسه: هل المحكمة المختصة بمحاكمة المتهم هي المحكمة

---

[1] محمد حزيط، المرجع السابق، ص195.

[2] المرجع نفسه، ص20.

[3] ج ر 71.

التي يتواجد في دائرتها الجهاز الذي تم إدخال المعلومات منه؟ أم هي المحكمة التي يتواجد فيها الجهاز الخادم؟ أم أن الاختصاص يؤول إلى كل محكمة في أي منطقة أو دولة تظهر فيها تلك الرسائل غير المشروعة؟[1]

إن إعمال القواعد العامة، وخاصة معيار مكان وقوع الجريمة لا يخلو من بعض الصعوبات، ذلك أن هناك نوعين من الجرائم الإلكترونية، نوع يضم الجرائم البحتة لتقنية المعلومات من مثل الولوج أو البقاء غير المشروعين إلى STAD، وإتلاف المعلومات...ونوع يضم الجرائم الواقعة بطريق من طرق نظم المعلومات، من مثل القذف والسب عبر الانترنت، النصب وغسيل الأموال عن طريق الانترنت؛ فالنوع الأول من الجرائم، يقع النشاط الإجرامي على جهاز معين يلج إليه الفاعل أو يبقى فيه بطريقة غير قانونية، وعليه يمكن القول بأن الجريمة تقع في المكان نفسه الذي يقع فيه نظام الجهاز المعتدى عليه، ما دام أن الولوج أو البقاء قد حدثا في مكان تواجد الجهاز الآلي نفسه، إلا أنه من الوارد أن يكون الولوج أو البقاء عن بعد من جهاز متواجد في مكان آخر، حينها يجوز القول بأن الجريمة حدثت في مكان وجود الجهاز المعتدى عليه، وفي مكان وجود الجهاز الذي استعان به الفاعل للقيام بنشاطه غير المشروع (الولوج أو البقاء)، هذا المكان الثاني قد يقع في اختصاص دائرة المحكمة التي يقع في دائرتها الجهاز المعتدى عليه، ولا مشكلة قانونية في هذا الفرض، وقد يقع هذا المكان في دائرة اختصاص محكمة أخرى قد تكون إما داخل الدولة ذاتها أو خارجها، وفي هذه الحالة يؤول الاختصاص طبقا لمبدأ الإقليمية إلى محكمة الجهاز المعتدى عليه ومحكمة الجهاز الذي تم منه الولوج أو البقاء غير المشروعين.[2]

أما بالنسبة للنوع الثاني من الجرائم، وهي الجرائم التقليدية التي ترتكب بوسيلة من وسائل تقنية المعلومات فإن الأمر لا يخلو من بعض الصعوبات فيما يتعلق بتحديد المحكمة المختصة، وقد اعتبرت أحكام للقضاء الفرنسي وأخرى للقضاء الأمريكي، الجريمة مرتكبة في كل مكان تظهر فيه الرسائل المؤثمة محل البث.[3]

---

[1] غنام محمد غنام، المرجع السابق، ص204.

[2] غنام محمد غنام، المرجع السابق، ص206.

[3] شيماء عبد الغني، المرجع السابق، ص371.

لكن جانبا من الفقه يرى بأن إعمال القواعد العامة لتحديد المحكمة المختصة يؤدي إلى نتائج غير مقبولة، من ذلك أن المحكمة التي يقع في دائرتها جهاز الخادم تختص بمحاكمة المتهمين عن كل الجرائم التي تقع بطريق الانترنت، كما هو الحال بالنسبة للطرد الناسف الذي يمر في أكثر من دولة أو في دائرة أكثر من محكمة في البلد الواحد، أو بالنسبة للجرائم التي تشكل العلانية ركنا فيها عندما تتحقق تلك العلانية بطريق الانترنت، لذلك بات من الضروري تنظيم المشرع لهذه المسألة بنصوص خاصة.[1]

المعول عليه وفق القواعد العامة في تحديد مكان وقوع الجريمة وبالتالي المحكمة المختصة، هو التمييز بين الجرائم المستمرة والجرائم المؤقتة، وهذا التمييز يكون حسب القواعد العامة وفقا لطبيعة النشاط الإجرامي، فالسرقة والنصب وخيانة الأمانة جرائم مؤقتة، أما حيازة الأشياء المسروقة أو إخفاؤها فتعد من الجرائم المستمرة، وبناء عليه، فإن الاختصاص في الجرائم المؤقتة ينعقد لمحكمة معينة، وهي التي وقع النشاط أو النتيجة في دائرة اختصاصها، ولا يلتفت إلى الأثر الذي تخلفه هذه الجريمة لأنه ليس من أركانها، أما الاختصاص في الجرائم المستمرة فينعقد لكل محكمة تتوافر في دائرتها حالة الاستمرار.[2]

[1] غنام محمد غنام، المرجع السابق، ص209.

[2] غنام محمد غنام، المرجع السابق، ص227-228.

المطلب الثاني: سلطة المحكمة المختصة في قبول وتقدير الدليل في مجال التجارة الإلكترونية.

يتم التطرق لهذا المبحث من خلال سلطة القاضي الجزائي في قبول الدليل الإلكتروني (الفرع الأول)، ثم سلطته في تقدير هذا الدليل (الفرع الثاني).

الفرع الأول: سلطة القاضي الجزائي في قبول الدليل الإلكتروني.

الدليل الإلكتروني من أهم الأدلة التي يلجأ إليها لإثبات الجرائم الواقعة على التجارة الإلكترونية، ويعد قبول الدليل الخطوة الإجرائية الأولى في مرحلة المحاكمة، قبل البدء في تقديره للتأكد من مدى صلاحيته وملاءمته لما قدم من أجله، واحترامه لمبدأ المشروعية.

أولا: أساس قبول الدليل الإلكتروني في الإثبات الجزائي.

يخضع هذا الأساس إلى طبيعة نظام الإثبات السائد في الدولة، والإثباتُ في المواد الجزائية يخضع لقواعد تختلف عن تلك التي تحكم الإثبات في المواد المدنية، وذلك لاعتبارات قد ترجع إلى اختلاف موضوع الإثبات بين تلك المواد ومنها ما يرجع إلى أهمية الدعوى الجزائية، وأن القواعد التي تحكم المسائل الجزائية تدور كلها حول غاية واحدة وهي الكشف عن حقيقة جريمة تمثل اعتداء على الجماعة وتهم المجتمع بأسره.

ومن القواعد التي تحكم الإثبات في المسائل الجنائية ثلاث: أولها حرية القاضي في تكوين عقيدته، بمعنى أن له أن يوجه تحقيقه في الجلسة بالشكل الذي يراه مناسبا وملائما للوصول إلى الحقيقة والكشف عنها دون أن يتقيد في ذلك باتباع وسائل معينة للكشف عن الحقيقة، كما أن له مطلق الحرية في تقدير أدلة الدعوى، فله أن يأخذ بها وله أن يطرحها، كل ذلك بناء على تقييمه لها وقناعته بما ينتهي إليه من مجموع ما طرح من أدلة في الجلسة، وأن يحكم في الدعوى حسب العقيدة التي تكونت لديه بكامل حريته مما يطرح أمامه على بساط البحث في الجلسة دون إلزام عليه بالتقيد بطريق معين من طرق الإثبات، إلا إذا أوجب القانون عليه ذلك، أو حظر عليه سلوك طريق معين في الإثبات، يستمد القاضي قناعته من أي ورقة سواء كانت رسمية أو عرفية يستخلص منها ما يطمئن إليه ضميره ووجدانه ويطرح ما لا يطمئن إليه، شأنه في ذلك شأن سائر الأدلة الأخرى التي قد تطرح أمامه، ولعل ذلك راجع إلى أن الإثبات الجنائي يتعلق بوقائع مادية، أو معنوية لها طابع استثنائي، وليس متعلقا بإثبات

تصرفات قانونية،[1] ومن جهة ثانية كي يكون ذلك في مقابل قرينة البراءة، كي يكون هنالك توازن بين مصلحة الفرد والمجتمع؛[2] وثاني القواعد التي تحكم لإثبات في المسائل الجزائية الدور الإيجابي للقاضي الجزائي في البحث عن الحقيقة، فإنه ليس مجرد موازن للأدلة المثبتة للإدانة أو البراءة، وإنما عليه التحري عن الحقيقة والكشف عنها، وهو في ذلك يختلف عن القاضي المدني الذي يكون دوره في الدعوى المدنية المنظورة أمامه سلبيا ومقتصرا على الموازنة بين أدلة الخصوم؛ وآخر القواعد التي تحكم الإثبات في المسائل الجزائية قاعدة عبء الإثبات في المواد الجزائية يقع على سلطة الإدعاء من منطلق أن الأصل في الإنسان البراءة، وعلى من يدعي عكس ذلك إثباته.[3]

ولا شك في أن مجموع هذه القواعد لا اختلاف فيها بين الجرائم التقليدية والجرائم الإلكترونية، إلا أن الطابع الخاص الذي تتميز به الجرائم الإلكترونية هو أن محل أو موضوع بعضها يكون غير مادي، إضافة إلى أن إثبات هذه الجرائم تحيط به الكثير من الصعوبات، تتمثل في صعوبة اكتشاف هذه الجرائم بحسب أنها جرائم فنية تتطلب تقنية معينة في مجال الحاسبات الآلية والإنترنت، وهي على الرغم من أنها – غالبا – ما تكون جريمة هادئة لا عنف فيها ولا تترك أشياء مادية تدرك بالحواس، لكونها عبارة عن أرقام وبيانات تتغير أو تمحى من السجلات المخزنة في ذاكرة الحاسبات، إلا أن البعض يشبهها بجرائم العنف مثل ما ذهب إليه مكتب التحقيقات الفيدرالي بالولايات المتحدة الأمريكية (FBI) نظرا لتماثل دوافع المعتدين على نظم الحاسب الآلي مع مرتكبي العنف.

وإلى جانب إمكانية ارتكاب هذه الجرائم خارج الحدود باستخدام شبكات الاتصال، فإن المجني عليه الذي عادة ما يكون مؤسسة مالية أو مشروعاً صناعياً ضخماً يحاول – في الغالب – كتم حصول الجريمة والإحجام عن البلاغ عنها أو مساعدة السلطات المختصة في إثباتها والكشف عنها حتى لا يتم تقليدها من قبل الآخرين، وخشية من أن يترتب على شيوع العلم بوقوعها إساءة واهتزاز لسمعته وثقة المساهمين والعملاء.

---

[1] د. محمد زكي أبو عامر، الإثبات في المواد الجنائية، دار الجامعة الجديدة، الإسكندرية، مصر 2011، ص108.

[2] المرجع نفسه، ص109.

[3] المرجع نفسه، ص100 وما بعدها.

ثانيا: خصائص ومميزات الدليل الإلكتروني

دليل الإثبات هو "الواقعة التي يستمد منها القاضي البرهان على إثبات اقتناعه بالحكم الذي ينتهي إليه "، والدليل الجنائي، معنى يدرك من مضمون واقعة تؤدي إلى ثبوت الإدانة أو استقرار البراءة، ويتم باستخدام الأسلوب العقلي وإعمال المنطق في وزن تقدير تلك الواقعة ليصبح المعنى المستمد منها أكثر دقة في الدلالة على الإدانة أو البراءة، وقد تعارف الفقه والقضاء على الأدلة التي يمكن للقاضي الاستناد إليها دون أن يحول ذلك عن الاستناد إلى أدلة أخرى.[1]

مع التطور التكنولوجي ظهر ما يسمي بالدليل الرقمي، أو الدليل الإلكتروني، و هو ما يعرف بأنه "الدليل الذي يجد له أساساً في العالم الافتراضي إلى الجريمة.

وعرف أيضا بأنه "الدليل المأخوذ من أجهزة الحاسب الآلي في شكل مجالات ونبضات مغناطيسية أو كهربائية ممكن تجميعها وتحليلها باستخدام برامج و تطبيقات و تكنولوجية خاصة.[2]

والدليل الرقمي هو مكون رقمي لتقديم معلومات في أشكال متنوعة مثل الرموز والنصوص المكتوبة أو الصور أو الأصوات والأشكال والرسوم يعبر عن فكر وقول يطلق عليه الكتابة الرقمية بالمعني الواسع، التي لا تشمل الكتابة التقليدية علي الورق فحسب، و إنما تشمل أيضا الكتابة التي تتم عن طريق وسائل الاتصال الحديثة، مهما كانت الدعامة المستخدمة في تثبيتها .

وللدليل الرقمي ثلاث خصائص، الأولى أنه دليل غير ملموس، والثانية أنه دليل من قبيل الأدلة الفنية أو العلمية، والخاصية الثالثة أن فهم مضمون الدليل الرقمي يعتمد على استخدام أجهزة تجميع وتحليل فحواه ليكون دليل إثباتها.

والأصل أن الدليل الرقمي غير مادي، يتكون من بيانات ومعلومات ذات هيئة رقمية غير ملموسة وإخراجه في شكل مادي ملموس يتطلب الاستعانة بأجهزة الحاسب الآلي وأدواته واستخدام نظم برمجية حاسبية ويتميز بالسرعة والسهولة وصعوبة محوه أو تحطيمه وإن حاول الجاني محو الدليل الرقمي، فإن هذه المحاولة بذاتها تسجل عليه كدليل، كما أن الطبيعة الفنية للدليل الرقمي تكمن في

[1] محمد زكي أبو عامر، المرجع السابق، ص119 وما بعدها.

[2] ممدوح عبد المجيد عبد المطلب ، استخدام بروتوكول TCP/IP في بحث و تحقيق الجرائم علي الكمبيوتر ، بحث منشور على الإنترنت.

إخضاعه لبعض البرامج والتطبيقات للتعرف على ما إذا كان قد تعرض للغش والتحريف، هذا من ناحية الجانب الايجابي، أما من حيث الجانب السلبي، فإن ذلك يتمثل في الاستخدام غير المشروع أو غير المصرح به للحاسب الآلي والانترنت وما عرف بالجرائم الإلكترونية وما يكتنف ذلك من مشكلات على المستوى التنظيمي والقانوني والتقني، الأمر الذي يتطلب وسائل تقنية وقواعد قانونية تحيطه بسياج من الحماية وهو ما أدى إلى صدور العديد من التشريعات كمحاولة لوضع ضوابط وتنظيم قانوني بقصد توفير الحماية اللازمة للمستخدمين والقائمين على تقديم خدمة الإنترنت .

وللدليل الرقمي ثلاثة أنواع : الأول مخرجات ذات طبيعة ورقية، تسجل فيها المعلومات على الورق، ويستخدم في ذلك الطابعات والراسم في طباعة الرسومات بدرجات وضوح مختلفة على الورق؛ النوع الثاني مخرجات ذات طبيعة إلكترونية، تستخدم في تخزين المعلومات بدل الوثائق الورقية كالأشرطة المغناطيسية والأوراق المغناطيسية؛ والنوع الثالث مخرجات مرئية معروضة بواسطة شاشة الحاسب الآلي ذاته ويتمثل هذا النوع في عرض البيانات المعالجة آليا بواسطة الحاسب الآلي على الشاشة الخاصة به.[1]

أما عن أنواع الدليل الرقمي كدليل إثبات من عدمه يمكن تقسيمه لنوعين رئيسين: أدلة أعدت لتكون وسيلة إثبات كالسجلات التي تم إنشائها بواسطة الآلة تلقائيا كذلك السجلات التي جزء منها تم حفظه بالإدخال وجزء تم إنشاؤه بواسطة الآلة، وأدلة لم تعد لتكون وسيلة إثبات وهذا النوع من الأدلة الرقمية ينشأ دون إرادة الشخص أي أنه أثر يتركه الجاني دون أن يكون راغبا في وجوده.

وتبدو أهمية التمييز بين هذين النوعين أن النوع الأول من الأدلة الرقمية هو الأكثر أهمية من النوع الثاني لكونه أعد أصلا ليكون وسيلة إثبات لبعض الوقائع، وعادة ما يعمد إلى حفظه للاحتجاج به لاحقا، بينما النوع الثاني من الأدلة الرقمية لم يعد أصلا ليكون أثرا لمن صدر ضده.

أما عن أشكال الدليل الرقمي فيمكن إيجازها في ثلاثة أشكال رئيسة: الصور الرقمية، التسجيلات، النصوص المكتوبة.

[1] وقسمت وزارة العدل الأمريكية عام 2002 الدليل الرقمي إلي ثلاث مجموعات هي : السجلات المحفوظة في الحاسب الآلي ؛ و السجلات التي يتم إنشاؤها بواسطة الحاسب الآلي و مخرجات برامجه التي لم يساهم الإنسان في إنشائها كسجلات الهاتف و فواتير أجهزة الحاسب الآلي؛ و النوع الثالث هو السجلات التي تم حفظ جزء منها بالإدخال و الجزء الأخر تم إنشاؤه بواسطة الحاسب الآلي و من أمثلة ذلك البيانات التي يتم إدخالها إلي الجهاز و تتم معالجتها من خلال برنامج خاص كإجراء العمليات الحسابية علي تلك البيانات .

ثالثا: القيمة القانونية للدليل الإلكتروني

القيمة القانونية للدليل الإلكتروني في مجال الإثبات الجنائي تتمثل في مشروعية الدليل الإلكتروني وحجيته، بحيث يمكن القول بأن النظم القانونية تختلف في موقفها من الأدلة التي تقبل كأساس للحكم بالإدانة، فهناك اتجاهان رئيسيان: الأول نظام الأدلة القانونية بمعنى أن المشرع يحدد الأدلة التي يجوز للقاضي اللجوء إليها في الإثبات، كما يحدد القيمة الاقناعية لكل دليل، فلا سبيل للاستناد إلى أي دليل لم ينص القانون عليه صراحة ضمن أدلة الإثبات، كما أنه لا دور للقاضي في تقدير القيمة الاقناعية للدليل، ولذا يسمى هذا النظام بنظام الإثبات القانوني أو المقيد، ويسود هذا النظام في الأنظمة الأنجلوسكسونية ؛ أما عن الثاني (نظام الإثبات الحر) فهو يسود في ظل الأنظمة اللاتينية، ووفقا لهذا النظام يتمتع القاضي الجنائي بحرية مطلقة في إثبات الوقائع المعروضة عليه، فلا يلزمه القانون الاستناد إليها في تكوين قناعته، أي أن الأصل في هذا النظام مشروعية وجوده، فالدليل الرقمي سيكون مشروعا من حيث الوجود استصحابا للأصل.

وقد تبنت بعض التشريعات نظام الإثبات المقيد أو ما يعرف بنظام الأدلة القانونية مع تمتع القاضي بسلطة واسعة في تقدير الدليل، والبعض الآخر من التشريعات تبنى نظام الأدلة القانونية الحرة.

إن تمتع الأدلة الرقمية بحجية قاطعة في الدلالة على الوقائع التي يتضمنها، من عدم ذلك مشكلة يمكن التغلب عليها من خلال إخضاع الأدلة الرقمية لاختبارات تمكن من التأكد من صحتها، ويرى البعض أنه لا يمكن اعتبار هذه القيمة المدعى بها للدليل الرقمي بمثابة خروج مستحدث عن القواعد العامة للإثبات في القانون الجنائي، حيث أن هناك من الأدلة ما لا يستطيع القاضي الجنائي تقديرها وفقا لسلطته المقررة، ويرى أصحاب هذا الرأي عدم الخلط بين الشك الذي يشوب الدليل الرقمي بسبب إمكانية العبث به أو لوجود خطأ في الحصول عليه، وبين القيمة الإقناعية لهذا الدليل، فالحالة الأولى لا يملك القاضي الفصل فيها لأنها مسألة فنية، فالقول فيها هو قول أهل الخبرة، فإن سلم الدليل الرقمي من العبث والخطأ، فإنه لن يكون للقاضي سوى القبول بهذا الدليل ولا يمكنه التشكيك في قيمته التدليلية لكونه وبحكم طبيعته الفنية يمثل إخباراً صادقاً عن الواقع ما لم يثبت عدم صلة الدليل بالجريمة المراد إثباتها.[1]

[1] طارق محمد الجملي، المرجع السابق.

ونتيجة تردد الفقه والقضاء حيال مشروعية الأدلة المتحصلة من الوسائل الإلكترونية كمخرجات الحاسب الآلي بأنواعها المختلفة، خشية أن تكون قد تعرضت للتغيير في فحواها أو لطمس الحقيقة فيها، خاصة أن معظمها يمس مساسا مباشرا بحقوق الأفراد الأساسية وحرياتهم، ولهذا وضعت شروط ينبغي توافرها في كل دليل مقدم أمام القضاء الجنائي كأن يكون الدليل مشروعا أي أن يكون وليد إجراءات صحيحة، وأن يكون قد طرح في الجلسة، وأن يكون مبنيا على الجزم واليقين.

وقد نصت بعض التشريعات المقارنة على بعض الشروط والضوابط التي يجب مراعاتها في مخرجات الحاسب الآلي لكي يمكن قبولها كأدلة إثبات من أهمها: أن يتم تحديد هوية الشخص أو الجهة المنسوب إليه المخرجات بصورة قاطعة؛ وأن يتم أيضا استخلاص المعلومات المخزنة إليكترونيا وحفظها بصورتها الأصلية التي أنشئت عليها وبصورة تضمن عدم تعرضها لأي شكل من أشكال العبث أو التلف،[1] وهذا الشرط يتطلب اتخاذ بعض الإجراءات التي من أهمها: التحقق من سلامة الحاسب الآلي ودقته في عرض المعلومات المخزنة، وحفظ مخرجات الحاسب الآلي وتخزينها في بيئة مناسبة، وكفاءة ونزاهة القائمين على جمع الأدلة وتخزينها .

وقد اعترفت بعض التشريعات بالدليل الكتابي الإلكتروني أو الرقمي، فنجد قانون الأمم المتحدة النموذجي للتجارة الإلكترونية يعترف بالدليل الكتابي الرقمي موضحا أنه في حالة ما إذا اشترط القانون أن تكون المعلومات مكتوبة فإنها تستوفى مثل هذه الشروط متى أمكن تخزينها والاطلاع عليها عند الحاجة لذلك، كما اعترف بعض تشريعات الدول بدليل الكتابي الرقمي،[2] واشترط الفقه أن تتوافر مجموعة شروط حتى يضطلع الدليل الكتابي الرقمي بدوره في الإثبات، و من هذه الشروط ضرورة أن يكون الدليل الكتابي مقروءاً و متصفاً بالاستمرار وغير قابل للتعديل.

وإذا كان التطور التقني في الوقت الحاضر أدي إلي تردد جانب من الفقه والقضاء حيال الأخذ بالكتابة الرقمية واستخدامها في المجال الجنائي كدليل شأنها في ذلك شأن المحررات الورقية في

[1] وقد أكدت ذلك المادة الثامنة من قانون الأونستيرال النموذجي الخاص بالتجارة الإلكترونية ، والمادة 1/1316 من القانون المدني الفرنسي، والمادة 3/1001 من قانون الإثبات الأمريكي، وتضمنت المادة الثامنة من قانون إمارة دبي للمعاملات التجارية الإلكترونية عدة شروط في هذا الخصوص.

[2] مثل المادة 2 من قانون المعاملات الإلكترونية لإمارة دبي و المادة 1 فقرة ب من قانون التوقيع الإلكتروني المصري و المادة 453 من القانون المدني التونسي رقم 57 لسنة 2000 و كذلك الفصل الرابع من القانون التونسي رقم 83 لسنة 2000 بشأن المعاملات الإلكترونية وأيضا نص المادة 92 من قانون البنوك الأردني رقم 28 لسنة 2000 .

الإثبات، على اعتبار أن هذا النوع من الجرائم له طبيعة خاصة نظراً لما تتميز به من تقنية عالية وخفاء في ارتكابها حيث يستطيع الجاني أن يرتكبها بسرعة دون أن يترك وراءه أي أثر خارجي ملموس لكونه يتميز عادة بالذكاء والدهاء والخبرة والمهارة التقنية العالية، كما أن هذا النوع من الكتابة له نتائج غير مؤكدة وأن معظمها يمس مساساً مباشراً بحقوق وحريات الأفراد الأساسية التي أقرها القانون في مراحل الدعوى الجنائية، لكن هذا التردد وما قد يثار من صعوبات ينبغي أن لا يقف حاجزا يمنع استفادة الأجهزة الضبطية والقضائية من التقنية الإلكترونية التي يقوم الجناة بتوظيفها في ارتكاب جرائمهم، والتعامل معهم باستخدام التقنية ذاتها في ملاحقتهم، بمعنى أن تقبل مستخرجات الحاسب الآلي كدليل من ضمن الأدلة الخاصة إذا ما توافرت فيها شروط وضوابط معينة، وهذا ما تأخذ به بعض التشريعات ومنها قانون التوقيع والتوثيق الإلكترونيين الجزائري.

الفرع اثاني: سلطة القاضي الجزائي في تقدير الدليل الإلكتروني.

يقتضي الأمر التطرق إلى نقطتين: نطاق سلطة القاضي الجزائي في تقدير الدليل الالكتروني، والضوابط التي تحكم اقتناع القاضي بالدليل الالكتروني.

أولا: نطاق سلطة القاضي الجزائي في تقدير الدليل الالكتروني.

الوصول إلى الحقيقة والكشف عنها هدف كل نظام إثبات في العالم من خلال تقدير الأدلة المعتمدة في الواقعة والمعروضة على القضاء، والسؤال المطروح: هل للقاضي كامل الحرية في تقدير هذه الأدلة وفق قناعته الشخصية؟ أم أن قيمتها التقديرية محددة سلفا من قبل المشرع، بحيث يكون القاضي ملزما بها، وليس له سوى تقدير قيمتها إن توافرت لديه القناعة القضائية؟[1]

يعد مبدأ الاقتناع القضائي من أهم المبادئ التي تقوم عليها نظرية الإثبات في المواد الجزائية، وقد تعددت الآراء حول مدلول الاقتناع القضائي، إلا أنها تلتقي في نقطة واحدة وهي أن للقاضي أن يستمد عقيدته من أي دليل يطمئن إليه، سواء من الأدلة المطروحة عليه من قبل النيابة العامة أو من قبل أحد الخصوم أو التي يرى تقديمها بنفسه، ليكون منها قناعته في الحكم، ولقد أقرت

[1] د. إدريس النوازلي، الإثبات الجنائي لجرائم الأعمال بالوسائل الحديثة، ج2، دار الآفاق المغربية للنشر والتوزيع، مراكش، المغرب 2014، ص191.

معظم التشريعات الحديثة هذا المبدأ حيث نص عليه المشرع الجزائري بنص م212 ق ا ج والمشرع المصري في م1/302 ق ا ج م، وقبلهما المشرع الفرنسي.[1]

لقد ثار خلاف حول نطاق تطبيق المبدأ المذكور سواء من حيث طبيعة القضاء أو من حيث مراحل الدعوى العمومية، ويمكن القول أن المبدأ يمتد تطبيقه إلى كافة أنواع المحاكم الجزائية، وإن لم ينص على ذلك صراحة كل من المشرعين الجزائري والمصري، على خلاف المشرع الفرنسي الذي نص على تطبيق المبدأ سواء أمام محكمة الجنايات أو الجنح أو المخالفات، ويمكن القول أيضا أن المبدأ شرع أصلا لقضاة الحكم، إلا أن الفقه يرى جواز امتداده لمرحلة التحقيق الابتدائي، ويستشف ذلك من نص م2/162 وم1/163 ق ا ج.

يثير الدليل الإلكتروني العديد من المشكلات تتعلق بطبيعته التكوينية من جهة وبإجراءات الحصول عليه من جهة أخرى، فالدليل الإلكتروني غير مرئي فهو عبارة عن نبضات إلكترونية مكونة من سلسلة طويلة من الأرقام الثنائية (الصفر والواحد) لا تفصح عن شخصية معينة، كما أن الدليل الإلكتروني غالبا ما يكون مرمزا ومشفرا، كما أن الأصالة في هذا الدليل مفترضة فقط، كما أن الدليل الإلكتروني ذو طبيعة متحركة يصعب معها تعقبه، كما أن الدليل الإلكتروني من الناحية الفنية يثير الكثير من الإشكاليات منها ارتفاع تكاليف الحصول عليه، ونقص المعرفة الفنية لدى رجال إنفاذ القانون.

إن الدليل الإلكتروني دليل علمي يجب لزوم تجاوبه مع الحقيقة كاملة وفقا لقاعدة في القضاء المقارن، هي قاعدة أن القانون مسعاه العدالة، أما العلم فمسعاه الحقيقة، لذلك يجب ألا يتعارض الدليل الإلكتروني مع القاعدة العلمية السليمة.[2]

ثانيا: الضوابط التي تحكم اقتناع القاضي الجزائي بالدليل الإلكتروني.

يتمتع القاضي الجزائي بسلطة واسعة في تقديره للأدلة والدليل الإلكتروني ليس مستثنى من هذه القاعدة العامة، غير أن المشرع وضع ضوابط كي لا ينحرف القاضي عن جادة الصواب عند ممارسته لهذه السلطة، وفيما يخص الدليل الإلكتروني فلا بد أن يكون هذا الدليل مقبولا، أي يحصل به اليقين في ضمير القاضي، بحيث تتطابق حالة الذهن والعقل مع حالة الواقع والحقيقة، ذلك أنه من

[1] عائشة بن قارة، المرجع السابق، ص240-244.

[2] النوازلي، المرجع السابق، ص201.

مقتضيات مبدأ أو قرينة البراءة أن يبنى الحكم الجزائي على الجزم واليقين لا على مجرد تخمين أو اتباع الظن،[1](وإن الظن لا يغني من الحق شيئا)، لذلك ليس معنى القول أن القاضي يملك حرية تقدير الأدلة بما فيها الأدلة الإلكترونية أو الرقمية أنه يملك الحكم بالإدانة على غير أساس من التثبت والتيقن، لكن هذا لا يمنع القاضي أن يؤسس حكمه بإدانة المتهم بترجيح فرض على آخر، إذ يكون هنا اقتناع القاضي بوقوع الجريمة ونسبتها إلى المتهم يقينا، لا يقدح فيه أن تستخلص المحكمة من الأدلة من مجموعها احتمالات متعددة لكيفية وقوع الجريمة، طالما أن جميع الاحتمالات تؤدي إلى إدانة المتهم، وليس هنالك ولو احتمال واحد يفيد البراءة، يرجح كفة البراءة اعتمادا على مبدأ "الشك يفسر لصالح المتهم".[2] وعليه فإن الحكم بالإدانة يجب أن يبنى على اليقين في صحة أدلة الإثبات، بينما يكفي في الحكم بالبراءة مجرد الشك، غير أن محكمة النقض الفرنسية لا تأخذ بمبدأ الشك يفسر لصالح المتهم إلا في أضيق نطاق، إذ أنها تعتبر أن مجرد وجود شك في الإدانة لا يكفي لتبرئة ساحة المتهم، بل يجب أن يستند هذا الشك على أدلة قاطعة.[3] وبالنسبة للأدلة الإلكترونية لا مجال لتطبيق ما توصلت إليه محكمة النقض الفرنسية فلا بد من أن تكون الأدلة الإلكترونية يقينية.

يجب أيضا مناقشة الأدلة الرقمية بطريقة شفوية أمام أطراف الدعوى وبحضورهم، ويجب على الخبير المعين من قبل المحكمة الحضور وتلاوة تقريره في الجلسة، فكل دليل مهما كان لا بد أن يخضع للمناقشة العلنية، وعليه فإن القاضي لا يجوز له أن يؤسس اقتناعه إلا على العناصر الإثباتية التي طرحت في جلسات المحاكمة وخضعت لحرية مناقشة أطراف الدعوى، ونصت على هذه القاعدة القوانين الإجرائية المقارنة.[4] غير أن هذا لا يعني أن القاضي لا يستند إلى ما ورد في التحقيقات الأولية التي قامت بها النيابة أو قاضي التحقيق، ويعتمد على الأدلة التي قدمت ضد المتهم دون سماعها، طالما أن هذه الأدلة كانت مطروحة للمناقشة بالجلسة.[5]

يترتب على مبدأ وجوب مناقشة الأدلة بما فيها الأدلة الرقمية فكرة عدم جواز أن يقضي القاضي في الجرائم المتعلقة بتقنية المعلومات بناء على معلوماته الشخصية أو على ما رآه بنفسه أو

---

[1] د. هلالي عبد اللاه أحمد، حجية المخرجات الكمبيوترية في المواد الجنائية، دراسة مقارنة، دار النهضة العربية، القاهرة 1997، ص85.

[2] د. هلالي عبد اللاه أحمد، المرجع السابق، ص87.

[3] المرجع نفسه، ص89.

[4] المرجع نفسه، ص99-108.

[5] المرجع نفسه، ص109.

حققه في غير مجلس القضاء وبدون حضور الخصوم، ولكن هذا لا يعني أن القاضي يكون له دور سلبي، كلا، فمن واجبه البحث عن الدليل ولكن في نطاق إجراءات الدعوى؛ كذلك يترتب عن المبدأ السابق فكرة عدم جواز أن يقضي القاضي في الجرائم الإلكترونية وغيرها بناء على رأي الغير، كأن يعتمد القاضي على أدلة وقائع استقاها من أوراق قضية أخرى لم تكن مضمومة للدعوى المنظور فيها، ولا مطروحة على بساط البحث بالجلسة تحت نظر الخصوم، غير أن هذا لا يعني حرمان القاضي من أن يأخذ برأي الغير متى اقتنع به وكان من الأدلة المقدمة إليه في الدعوى محل نظره، ويتعين عليه في هذه الحالة تبيان أسباب اقتناعه بهذا الرأي.[1]

تواترت محكمة النقض المصرية على أن يكون استخلاص محكمة الموضوع لواقعة الدعوى استخلاصا معقولا تؤدي إليه ظروف الواقعة وأدلتها وقرائن الأحوال فيها.[2]

[1] هلالي عبد اللاه أحمد، المرجع السابق، ص115.

[2] عائشة بن قارة، المرجع السابق، ص281.

الفصل الثاني: التعاون الدولي لمكافحة الجرائم الواقعة على التجارة الإلكترونية.

التعاون الدولي عبارة عن تبادل العون والمساعدة وتضافر الجهود المشتركة بين دولتين أو أكثر، لتحقيق نفع أو خدمة مشتركة، سواء أكانت على مستوى عالمي أو على مستوى إقليمي، أو على المستوى الوطني للدول التي يتم الاتصال فيما بينها.[1]

وعادة ما ينشأ التعاون الدولي نتيجة اختلاف العوامل التاريخية وتباين الأنظمة الخاصة لكل دولة، إذ تلجأ الدول للاتفاق على حدود وأوضاع معينة بغية مكافحة الجريمة، لإدراك الدول التام بأن مواجهة الجريمة وخاصة تلك العابرة للحدود مهمة الجميع وفيه مصلحة للجميع، ويحتاج إلى التعاون، خاصة وأن هذه الجرائم تعرف تطورا مستمرا وتهدد مصالح كل الدول الاقتصادية والسياسية والاجتماعية.[2]

بخصوص الجرائم الإلكترونية، وخاصة تلك التي ترتكب عبر شبكة الانترنت، لم يكن هناك قلق دولي مع بدايات هذه الشبكة من جرائم يمكن أن ترتكب عليها أو بواسطتها، لا لأنها آمنة في تصميمها وبنائها، بل نظرا لمحدودية مستخدميها، علاوة على أنها كانت مقصورة على فئة معينة من المستخدمين، إلا أنه ومع توسع استخدامها ودخول جميع فئات المجتمع إلى قائمة مستخدميها وتطور التقنيات، بدأت تظهر إلى الوجود ما يسمى بالجرائم المعلوماتية، خاصة على شبكة الانترنت أو بواسطتها، وكذا بواسطة جميع الوسائل الإلكترونية الأخرى المتطورة من حاسب آلي عادي ومحمول، وأجهزة الهاتف النقال الذكية وغيرها... هذه الجرائم تتميز بحداثة الأسلوب وسرعة التنفيذ وسهولة الإخفاء والقدرة على محو آثارها وتعدد صورها وأشكالها؛ ليس هذا فحسب بل اتصفت بالعالمية وبأنها عابرة للحدود، وهذا أمر طبيعي خاصة إذا ما علمنا أن شبكة الانترنت ذاتها لا تعرف الحدود، فهي ذات طبيعة عالمية.

وإزاء ذلك كله كان لا بد من تكاتف جهود الدول من أجل مكافحة هذا النوع المستحدث من الجرائم التي لم تعد تتمركز في دولة معينة ولا توجه لمجتمع بعينه، بل أصبحت تعبر

[1] معادي أسعد، المرجع السابق، ص472.

[2] المرجع نفسه، ص473.

الحدود[1] لتلحق الضرر بعدة دول ومجتمعات، مستغلة التطور الكبير للوسائل التقنية الحديثة في الاتصالات ونظم المعلومات.

من أجل التصدي للجرائم الواقعة على التجارة الإلكترونية بصفة خاصة، والجرائم الإلكترونية عامة، فإنه لا مفر من التعاون وتضافر الجهود الدولية، ورسم رؤية شاملة وموحدة، تهدف إلى التكامل بين مختلف الفواعل الوطنية والدولية، وتوفير كل وسائل الحماية سواء أكانت قانونية أم فنية أم غيرها.

ونظرا لخطورة الجرائم الإلكترونية، وأهمية التعاون الدولي، فقد بذلت المنظمات الدولية مجهودات معتبرة، من ذلك، وضع القوانين النموذجية للتجارة الإلكترونية والتوقيع الإلكتروني، والاهتمام بمواضيع الملكية الفكرية وأسماء النطاق، كما أفرد مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاملة المجرمين إحدى حلقاته الأربع الواردة على جدول أعماله لدراسة الجرائم المتصلة بالحاسب الآلي وشبكة الانترنت، حيث أشير خلال المناقشات أن هذه الجرائم هي جرائم عبر وطنية، تمثل إحدى تحديات القرن الحادي والعشرين.[2]

---

[1] هناك من يصف جرائم نظم المعلومات بأنها جرائم دولية لأنها عابرة للحدود، والحقيقة أن هذا الوصف غير دقيق، والأصح أن توصف بالجرائم العالمية، حيث يقصد بالجريمة العالمية الأفعال التي تنطوي على عدوان على القيم البشرية والأخلاقية الأساسية في العالم المتمدن مثل الحق في الحياة وسلامة الجسم والحرية والحياء العام، وهذه الأفعال تشكل جرائم عادية، نصت عليها أغلب التشريعات الجنائية، لما تمثله من عدوان على القيم الإنسانية كلها، وتتعاون الدول في مكافحتها، وأوصت المنظمات الدولية بعقد الاتفاقيات، وحث الدول على توحيد القواعد الموضوعية والإجرائية من أجل مكافحتها، وتعزيز التضامن بين الدول من أجل القضاء عليها، ومعاقبة مرتكبيها، وتدخل هذه الجرائم في إطار قانون العقوبات العالمي وليس القانون الدولي الجنائي، ولا تعد جرائم دولية، وإنما جرائم عادية ولو جاء النص عليها في اتفاق أو معاهدة دولية.

ورغم أن الجريمة العالمية يمكن أن ترتكب في أقاليم دول متعددة، لا ينفي عنها أنها جريمة يختص بالعقاب عليها القانون الداخلي وهو ما يميزها عن الجريمة الدولية التي يختص بنظرها القانون الدولي، فالجريمة الدولية تنطوي على العنصر الدولي الذي يتمثل في المساس بالمصلحة الدولية محل الحماية الجنائية الدولية، بينما الجريمة العالمية ليست جريمة دولية، وإنما هي جريمة عادية تم ارتكابها في عدة دول مما أضفى عليها صفة العالمية، ويعاقب عليها القانون الجنائي الدولي، بينما الجريمة الدولية يختص بالعقاب عليها القانون الدولي الجنائي،كما أن الجريمة الدولية يتطلب قيامها توافر ركن دولي، لا وجود له في الجريمة العالمية التي تعد جريمة وطنية عادية، ويترتب على هذا أن الجريمة العالمية قد تنقلب إلى جريمة دولية إذا توافر الركن الدولي، فجرائم تقنية المعلومات هي جرائم عالمية تعاقب عليها التشريعات الداخلية للدولة، وتتعاون الدول جميعا للحد من هذه الجرائم أو القضاء عليها، لكن هذه الجرائم إذا مارستها دولة ضد دولة أخرى، أو ارتكبها أفراد عاديون بتشجيع من الدولة أو بدعم منها اعتبرت في هذه الحالة جرائم دولية،كما أن الجريمة العالمية تخضع لمبدأ اختصاص القضاء الوطني فيطبق عليها القانون الداخلي للدولة، أما الجريمة الدولية فيسري عليها القانون الدولي الجنائي، وتختص بالمحاكمة عنها المحاكم الدولية أو المحاكم الوطنية. يراجع: محمد هشام فريجة، دور القضاء الدولي الجنائي في مكافحة الجريمة الدولية، أطروحة دكتوراه علوم في الحقوق، تخصص قانون جنائي، جامعة محمد خيضر، بسكرة 2014/2013، ص35.

[2] سامح أحمد، المرجع السابق، ص496.

انطلاقا مما سبق، يعالج هذا الفصل ضرورة التعاون الدولي في مجال محاربة الجرائم الواقعة على التجارة الإلكترونية (المبحث الأول)، ثم العقبات والمشاكل التي من الممكن أن تعترض التعاون الدولي في هذا المجال وسبل حلها (المبحث الثاني).

المبحث الأول: ضرورة التعاون الدولي في مجال مكافحة الجرائم الواقعة على التجارة الإلكترونية.

بدأ العالم يدرك، – وخاصة بعد انهيار المعسكر الشرقي، وظهور ما يسمى العولمة، وتطور الوسائل التقنية وثورة الاتصالات، وانفتاح العالم بعضه على بعض — أهمية التعاون لمجابهة الجرائم المستحدثة، وخاصة الجرائم العابرة للحدود، ومن أخطرها الجرائم الإلكترونية عامة، وجرائم التجارة الإلكترونية بصفة خاصة، وتزيد أهمية التعاون حينما ندرك أن المجرمين يتعاونون بينهم بوسائل شتى، ولدوافع مختلفة، ويستخدمون الوسائل المتطورة في إجرامهم، وهم بذلك يهددون أمن الدول واستقرارها الاقتصادي والسياسي والاجتماعي، ولذا بات من الضروري تغيير النظرة التقليدية لمفهوم السيادة، وتبني مفهوم آخر يقوم على السيادة النسبية للدول، من دون استغلال الأمر للتدخلات غير المبررة في شؤون الدول الداخلية، ولعل هذا ما تطرقت إليه مثلا م4 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، تحت عنوان صون السيادة حينما نصت بصريح العبارة على مبدأي المساواة في السيادة الإقليمية للدول وعدم التدخل في الشؤون الداخلية لدول أخرى، وأكدت هذين المبدأين بالنص صراحة بأن الاتفاقية ليس فيها ما يبيح لدولة طرف أن تقوم في إقليم دولة أخرى بممارسة الولاية القضائية، وأداء الوظائف التي يناط أداؤها حصرا بسلطات تلك الدولة الأخرى بمقتضى قوانينها الداخلية.

إن جرائم التجارة الإلكترونية غير إقليمية فهي عالمية في أغلب الأحيان، أي جرائم عبر وطنية، مما يجعل أركانها ونتائجها موزعة على عدة دول، كما أن أدلتها من نوع خاص، يسهل على البعض ممن يمتلكون الملكات والموهبة والخبرات الفنية محوها أو إخفاؤها، مما يشكل صعوبة بالغة للقوانين الوطنية التقليدية في التصدي لمثل هذه الجرائم وكشف مرتكبيها ومحاكمتهم ومعاقبتهم، تحقيقا للردع الخاص والردع العام معا، وحماية للثقة في التعاملات الإلكترونية، وهذا ما دفع المجتمع الدولي إلى التوجه شيئا فشيئا نحو إنشاء أجهزة تعاون دولي، تعمل على مستوى أجهزة حكومية أو غير

حكومية، من أجل ضمان التنسيق والمتابعة المشتركة وتبادل المعلومات وتسهيل الإجراءات قصد تحقيق الهدف المنشود، ألا يفلت المجرمون من العقاب.[1]

ولعل من أبرز مظاهر التعاون لمجابهة ومكافحة الجرائم العابرة للحدود ومنها الجرائم الواقعة على التجارة الإلكترونية، التعاونُ القضائي، والتعاون الدولي الأمني، وكذا تسليم المجرمين، بالإضافة طبعا إلى المساعدة غير الرسمية، والتي تكون أحيانا أسرع إنجازا، وهي الوسيلة المفضلة حين لا تكون هناك حاجة إلى صلاحيات إلزامية (أي أوامر تفتيش أو طلب تسليم المجرم)، وهي تقوم على وجود علاقات عمل جيدة بين أجهزة شرطة البلدان المعنية، وتتدعم نتيجة الاتصالات التي تجري مع الوقت في مسار المؤتمرات وزيارات المجاملة والتحقيقات المشتركة السابقة.

المطلب الأول: التعاون القضائي في مجال مكافحة الجرائم الواقعة على التجارة الإلكترونية.

يعتبر التعاون القضائي من أبرز مظاهر التعاون الدولي لمواجهة الجرائم المستحدثة بصفة عامة، والجرائم الواقعة على التجارة الإلكترونية بصفة خاصة، ويتخذ هذا التعاون عدة صور هي المساعدة القضائية، الإنابة القضائية، نقل الإجراءات الجزائية، والاعتراف بتنفيذ الأحكام الجزائية الأجنبية.

الفرع الأول: المساعدة القضائية الدولية.

يعالَج هذا الفرع من خلال التطرق إلى طبيعة المساعدة القضائية، وصورها، وشروط طلبها.

أولا: طبيعة المساعدة القضائية الدولية.

تشمل المساعدة القضائية في الاتفاقيات الدولية الحديثة صورا متعددة، وقد اتسع مجالها في الاتفاقية الأوربية الخاصة بالمساعدة القضائية في المواد الجزائية.

تتعلق المساعدة القضائية بالمعاونة في مجابهة الجرائم في المجال الجنائي، من خلال الاتفاقيات، مثل نقل صحف الحالة الجنائية، والمعاونة في المواد الجزائية من خلال تجميع عناصر

[1] سامح أحمد، المرجع السابق، ص499.

الأدلة، ونقل الإجراءات الجزائية القمعية، والتي تعني القيام بإجراءات جزائية بصدد جريمة ارتكبت في دولة أخرى ولحساب هذه الدولة.[1]

تشمل المساعدة القضائية في المسائل الجنائية مجالات متعددة أبرزها إجراءات التحقيق والمحاكمة وجمع الأدلة وضبطها وفحصها، وتنفيذ الأحكام، ونقل المحكوم عليهم.

بالنسبة للجرائم الواقعة على التجارة الإلكترونية، وكما سبق القول، فإنه يمكن أن تكون ذات صبغة عالمية، بل هذا هو الغالب عليها، وبالتالي فإن آثارها تتعدى حدود الدولة الواحدة، وعليه، يستلزم الأمر القيام بأعمال إجرائية خارج حدود الدولة التي ارتكبت بعض أركان الجريمة فيها، ومن هذه الأعمال ضبط الأقراص الصلبة التي قد تحوي معلومات تفيد في كشف الحقيقة، أو تفتيش الوحدات الطرفية في حال الاتصال عن بعد، أو القبض على المتهمين، أو سماع الشهود، أو اللجوء إلى الإنابة القضائية، أو تقديم المعلومات التي من شأنها أن تفيد في كشف هذه الجرائم.[2]

بناء على ما تقدم تعرّف المساعدة القضائية الدولية بأنها: "كل إجراء قضائي تقوم به دولة من شأنه تسهيل مهمة المحاكمة في دولة أخرى بصدد جريمة من الجرائم".[3]

على الصعيد الدولي، كان التعاون الدولي في مجال المساعدة القضائية الجنائية واردا ضمن إطار المعاهدات المتصلة بمكافحة نوعية معينة من الجرائم، دعت الضرورة إلى اتفاق دول العالم على مواجهتها بشكل جماعي موحد، مثل الاتفاقيات الخاصة بمكافحة المخدرات والمؤثرات العقلية، والاتفاقيات المختصة بالرقيق، وتلك الخاصة بمكافحة الاتجار بالبشر، والاتفاقيات الخاصة بالجرائم الإرهابية والاتفاقيات المتعلقة بالجريمة المنظمة وبعض الاتفاقيات المتعلقة بحقوق الإنسان، وغير ذلك من الاتفاقيات المهمة، وفيما يخص الاتفاقيات المتعلقة بالجرائم الإلكترونية، كانت هنالك جهود حثيثة من المجتمع الدولي لمحاربة هذا النوع من الجرائم من خلال المؤتمر السابع للأمم المتحدة المنعقد بميلانو سنة 1985، الذي كلف لجنة الخبراء العشرين بدراسة موضوع حماية نظم المعالجة الآلية، والاعتداء على الحاسب الآلي، وإعداد تقرير يتم عرضه على المؤتمر الثامن، الذي عقد في هافانا سنة

[1] د. أحمد عبد الحليم شاكر علي، دور الإنابة القضائية الدولية في مكافحة الجريمة، مجلة الفكر الشرطي، المجلد17، العدد4، 2008، ص153.
[2] سامح أحمد، المرجع السابق، ص500.
[3] المرجع نفسه، ص501.

1990 وخرج بالعديد من التوصيات، منها التعاون مع المنظمات المهتمة بالموضوع، كما عقد مؤتمر الأمم المتحدة لمنع الجريمة ومعاملة المجرمين في القاهرة سنة 1995، الذي أوصى بضرورة حماية حقوق الإنسان في حياته الخاصة، وملكيته الفكرية في مواجهة مخاطر التكنولوجيا الحديثة، ووجوب التنسيق والتعاون بين فواعل المجتمع الدولي، كما أوصى المؤتمر العاشر المنعقد في بودابست سنة 2000 بوجوب العمل الجاد من أجل الحد من جرائم تقنية المعلومات المتزايدة واتخاذ التدابير المناسبة والكفيلة بوقف أو الحد من أعمال القرصنة.[1]

وهناك اتفاقيات صادرة عن جامعة الدول العربية كتلك المتعلقة بتسليم المجرمين وتنفيذ الأحكام والإنابات القضائية، واتفاقية الرياض للتعاون القضائي التي اعتمدها مجلس وزراء العدل العرب في دورته الأولى بالقرار رقم 01 في1983/4/6، ودخلت حيّز النفاذ بتاريخ 1985/10/30،[2] واتفاقية التعاون القانوني والقضائي بين دول اتحاد المغرب العربي الموقعة بليبيا عام 1991،[3] والاتفاقية العربية لمكافحة جرائم تقنية المعلومات المحررة بالقاهرة بتاريخ 2010/12/21، والتي نص الفصل الرابع منها على التعاون القانوني والقضائي، وذلك من خلال المواد 32-43، كما أن هناك اتفاقيات أخرى من مثل الاتفاقيات الصادرة عن المجلس الأوربي بشأن المساعدة في المواد الجنائية.

أما على المستوى الوطني فإن القانون رقم 09-04 سالف الذكر تطرق في المادة 16 منه إلى موضوع المساعدة القضائية الدولية المتبادلة وأجازها في إطار التحريات أو التحقيقات القضائية الجارية لمعاينة الجرائم المذكورة حصرا في القانون 09-04 سالف الذكر وكشف مرتكبيها وجمع الأدلة الخاصة بالجريمة في الشكل الإلكتروني؛ بل أجاز المشرع الجزائري في الفقرة الثانية من المادة المذكورة آنفا في حالة الاستعجال قبول طلبات المساعدة القضائية حتى إذا وردت عن طريق وسائل الاتصال السريعة من مثل الفاكس والبريد الإلكتروني بقدر ما توفره هذه الوسائل من شروط أمن كافية للتأكد من صحتها، وهذا في إطار الاتفاقيات الدولية ومبدأ المعاملة بالمثل، ولا ترفض طلبات المساعدة القضائية الدولية إلا إذا كان من شأنها المساس بالسيادة الوطنية أو النظام العام (م18 من القانون رقم 09-04).

---

[1] نعيم سعيداني، المرجع السابق، ص84.

[2] صادقت عليها الجزائر بموجب المرسوم الرئاسي رقم 01-47 المؤرخ في 11 فبراير 2001، ج ر11 الصادرة في 12 فبراير 2001.

[3] صادقت عليها الجزائر بموجب المرسوم الرئاسي رقم 94-181 المؤرخ في 27 يونيو 1994، ج ر43 الصادرة في 03 يوليو 1994.

ثانيا: صور المساعدة القضائية الدولية.

من أبرز هذه الصور: تبادل المعلومات، تبادل صحف الحالة الجنائية، حضور الشهود والخبراء، وضمان حق التقاضي.

1- تبادل المعلومات.

يتعين حصول الدولة التي اتهم أحد مواطنيها في الخارج على المعلومات والوثائق التي تتعلق بالاتهامات الموجهة إليه والإجراءات التي تم اتخاذها ضده.[1]

يتم تبادل المعلومات بين الدول لفائدة التحقيق في الجرائم المرتبطة بالتجارة الإلكترونية، وهذا ما قررته اتفاقية بودابست لسنة 2001 حول الجرائم الافتراضية، وتحديدا في م23 التي تقرر صراحة وجوب التعاون الدولي بين الأطراف وتعميقه، وتقليل العوائق، بما يوفر أكبر قدر من السهولة والسرعة لتبادل المعلومات والأدلة بين الدول الأطراف.

نصت م1 من اتفاقية الرياض العربية للتعاون القضائي والتي صادقت عليها الجزائر على: "تتبادل وزارات العدل لدى الأطراف المتعاقدة بصفة منتظمة نصوص التشريعات النافذة والمطبوعات والنشرات والبحوث القانونية والقضائية، والمجلات التي تُنشر فيها الأحكام القضائية، كما تتبادل المعلومات المختلفة المتعلقة بالتنظيم القضائي، وتعمل على اتخاذ الإجراءات الرامية إلى التوفيق بين النصوص التشريعية، والتنسيق بين الأنظمة القضائية لدى الأطراف المتعاقدة، حسب ما تقتضيه الظروف الخاصة بكل منها".[2]

أما م32 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات سالفة الذكر فدعت الدول الأطراف على تبادل المساعدة فيما بينها بأقصى مدى ممكن، كما أكدت م33 من الاتفاقية ذاتها على هذا التعاون، من خلال جواز إعطاء معلومات من قبل دولة طرف في الاتفاقية حصلت عليها من خلال تحقيقاتها، حتى دون طلب هذه المعلومات من الدولة الأخرى، إذا رأت أن كشف مثل هذه المعلومات يمكن أن يساعد الدولة الطرف المرسلة إليها المعلومات في إجراء الشروع أو القيام بتحقيقات في الجرائم المنصوص عليها في الاتفاقية، أو قد يؤدي إلى طلب للتعاون من قبل تلك

[1] طارق فوزي، المرجع السابق، ص260.

[2] سامح أحمد، المرجع السابق، ص501.

الدولة الطرف، مع مراعاة الشروط الواردة في م2/33 والمتعلقة بسرية المعلومات المقدمة، كما نصت م18 من القانون 09-04 سالف الذكر على أحقية الدولة ألا تستجيب لطلبات المساعدة إلا بشرط المحافظة على سرية المعلومات المبلغة أو بشرط عدم استعمالها في غير ما هو موضح في الطلب.

2- تبادل صحف الحالة الجنائية.

يتم هذا التبادل عن طريق تقديم المساعدة القضائية الدولية في المجال الجنائي، ووفقا لما نصت عليه م5 من اتفاقية الرياض للتعاون القضائي فإن تبادل صحف (سجلات) الحالة الجنائية يتمثل في تبادل وزارتي العدل في أي دولتين متعاقدتين بيانات عن الأحكام النهائية الصادرة ضد مواطني إحدى الدولتين، أو الأشخاص المولودين أو المقيمين في إقليمها والمقيدين في صحف الحالة الجنائية، هذه البيانات تكشف عن السوابق الجنائية لهؤلاء الأشخاص.

بيد أن بعض الدول لا تجيز إعطاء مثل هذه الصحف الجنائية مثل فرنسا مثلا، حيث لا تسمح بإعطاء صور ضوئية من صحف الحالة الجنائية إلا عن رعايا الدول التي بينها وبين فرنسا اتفاقيات لتبادل المعلومات.

3- حضور الشهود والخبراء.

يمثل حضور الشهود والخبراء من دولة إلى أخرى صورة هامة من صور المساعدة القضائية الدولية في المجال الجنائي، ويشترط أن يحضر الشاهد أو الخبير طواعية أي دون إجبار، إلى الهيئات القضائية في الدولة التي تطلب حضوره، ويتمتع بحصانة ضد اتخاذ أية إجراءات جنائية بحقه، كالقبض عليه أو حبسه عن أفعال أو تنفيذ أحكام سابقة على دخوله إقليم الدولة طالبة حضوه، ويتعين إخطار الشاهد أو الخبير كتابة بهذه الحصانة قبل حضوره لأول مرة طبقا لنص م22 من اتفاقية الرياض العربية للتعاون القضائي، وحسب نص م19 من الاتفاقية ذاتها فإن تكليف الأشخاص المطلوب سماع شهاداتهم يتم بالطرق المتبعة لدى الطرف المطلوب أداء الشهادة لديه.

4- ضمان حق التقاضي.

حيث يتمتع مواطنو الدول الأطراف في اتفاقية ما بحق التقاضي أمام الهيئات القضائية للمطالبة بحقوقهم أو الدفاع عنها، ولا يجوز بأي حال كان أن تفرض عليهم أية ضمانة شخصية أو

عينية بأي وجه، لكونهم لا يحملون جنسية الطرف المتعاقد، أو لعدم وجود موطن أو محل إقامة لهم داخل حدوده، طبقا لنص م3 من اتفاقية الرياض العربية للتعاون القضائي سالفة الذكر.

ثالثا: طلب المساعدة القضائية.

يشترط في طلب المساعدة القضائية أن تكون الدولة طالبة المساعدة مختصة بنظر الدعوى الجنائية، حيث يتمثل هدف المساعدة القضائية الدولية في تسهيل ممارسة الاختصاص الجنائي للدولة، وليس مجرد ضمان الحضور الشخصي للمتهم، كما هو الحال في التسليم، ويتم تنفيذ المساعدة القضائية الدولية وفقا للقواعد والإجراءات المنصوص عليها، الواردة ضمن تشريع الدولة المطلوب منها المساعدة.[1]

تمثل الاتفاقيات الدولية السند القانوني الذي ترتكز عليه الدول المتعاقدة حال طلب إحداها مساعدة قضائية من أخرى، حسب ما تضعه كل اتفاقية من مبادئ وضوابط وشروط، وما ترسيه من قواعد؛ فقد نصت م2/23 من الاتفاقية الأوربية حول الجريمة المعلوماتية والمعروفة باتفاقية بودابست لسنة 2001، على ما يلي: "يمتد نطاق الالتزام بالتعاون الدولي في هذه المادة إلى كافة الجرائم المرتبطة بنظم الحاسب الآلي والبيانات..."

وقد لعبت الاتفاقيات الدولية الثنائية المتعلقة بالتعاون الدولي، في مجال المساعدة القضائية الدولية في المجال الجنائي، دورا هاما في اتساع نطاق المساندة، وابتكار سبل جديدة وعالة ي مواجهة المشاكل والصعوبات التي تظهر عند تطبيق الاتفاقيات، ومن أمثلة ذلك المعاهدةُ الموقعة بين الو م أ وسويسرا عام 1977 بشأن المخدرات وتبييض الأموال، والاتفاقية الموقعة بين مصر وسويسرا عام 2001 وغيرها من الاتفاقيات الثنائية.[2]

[1] سامح أحمد، المرجع السابق، ص503.

[2] سامح أحمد، المرجع السابق، ص503.

الفرع الثاني: الإنابة القضائية الدولية.

يعالج هذا الفرع من خلال التطرق إلى تعريف الإنابة القضائية الدولية، وإجراءات طلبها.

أولا: تعريف الإنابة القضائية الدولية.

تعرف الإنابة القضائية الدولية بأنها: "طلب تنتدب فيه المحكمة المرفوعة أمامها الدعوى محكمة وجود الشاهد، أو الأوراق، أو الشيء، أو تنيبها لعمل الإجراء اللازم، وتحرير محضر بذلك وإرساله لها بعد تمامه"،[1] أو "هي طلب اتخاذ إجراء قضائي من إجراءات الدعوى العمومية، تتقدم به الدولة الطالبة إلى الدولة المطلوب إليها، وذلك للفصل في مسألة معروضة على السلطة القضائية في الدول الطالبة التي يتعذر عليها القيام به بنفسها".[2]

تعبر الإنابة القضائية عن قيام دولة ما بمباشرة إجراء قضائي يتعلق بدعوى قيد النظر داخل الحدود الإقليمية لدولة أخرى نيابة عنها، بناء على طلب هذه الدولة المناب عنها، وفقا لما تقرره بنود الاتفاقية الدولية بين الدولتين في هذا الشأن.[3]

وتتميز الإنابة القضائية بين الدول في مجال مكافحة الجرائم الدولية بشكل عام، والجرائم الواقعة على التجارة الإلكترونية بشكل خاص، بمميزات هامة، تتمحور حول الحفاظ على السيادة الوطنية، حيث تقوم الأجهزة الأمنية المتخصصة بتلك الإجراءات المطلوبة على أرض الدولة، دون مشاركة حقيقية من الأجهزة الأمنية في الدولة الأخرى الطالبة.

يساعد تنفيذ هذا التعاون في الوقت المناسب على عدم ضياع الأدلة والآثار المتعلقة بالجريمة، وإنجاز التحقيقات الجارية في الدول الطالبة، ويحفظ أيضا حقوق المتهمين في الإسراع بمحاكمتهم وعدم بقائهم في الحبس المؤقت دون محاكمة انتظارا لإتمام تلك الإجراءات القانونية في دولة أخرى.[4]

---

[1] أحمد عبد الحليم، المرجع السابق، ص150.

[2] طارق فوزي، المرجع السابق، ص262.

[3] سامح أحمد، المرجع السابق، ص504.

[4] خالد بن مبارك القريوي القحطاني، التعاون الأمني الدولي في مواجهة الجريمة المنظمة عبر الوطنية، رسالة دكتوراه في الفلسفة في العلوم الأمنية، كلية الدراسات العليا، جامعة نايف العربية، الرياض 2006، ص63.

حددت م14 من اتفاقية الرياض العربية للتعاون القضائي مجالات الإنابة القضائية في مباشرة أي إجراء قضائي متعلق بدعوى قائمة وبصفة خاصة سماع الشهود وتلقي تقارير الخبراء ومناقشتهم، وإجراء المعاينة وطلب تحليف اليمين.

ثانيا: إجراءات طلب الإنابة القضائية الدولية.

هنالك تشابه كبير بين الإنابة القضائية الدولية والانتداب أو الأمر أو الإذن من قبل قاضي التحقيق وطنيا لضابط الشرطة القضائية المندوب في اتخاذ إجراء معين، ويكون هذا الإجراء كما لو تم تحت سلطة قاضي التحقيق، غير أن الفارق أن الإنابة الدولية تتم بين الجهات المختصة في دولتين مختلفتين، ناهيك عن أن الانتداب داخليا قد يكون من سلطة عليا إلى سلطة أدنى منها، وهو ما لا يتحقق في الإنابة القضائية الدولية.[1]

وتعني إجراءات الإنابة القضائية تلك الإجراءات الشكلية اللازمة في تنفيذ الإنابة، ويعبر عنها بطرق الإنابة بين جهتيها، وهما الجهة الطالبة والجهة المطلوب منها، وهي التي ستتولى تنفيذ تلك الإنابة.

هناك ثلاثة طرق لنقل الإنابة القضائية وهي:[2]

– الطريق الدبلوماسي: تقوم المحكمة القائمة بنظر الدعوى بإرسال طلب الإنابة إلى وزارة الخارجية، وتقوم هذه الأخيرة بإرسال الطلب ذاته إلى ممثلها الدبلوماسي في الدولة المطالبة بتنفيذ طلب الإنابة، ويطلق أحيانا على هذا الطريق "الطريق السياسي".

– الطريق القنصلي: يتم ذلك بأن تقوم المحكمة المختصة بإرسال الإنابة القضائية مباشرة إلى قنصل دولتها في البلد الأجنبي المطلوب منه تنفيذ الإنابة، هذا الأخير يقوم بتوجيه الإنابة إلى الجهة المختصة في الدولة القائمة بالتنفيذ.

– الطريق القضائي: يعرف هذا الأسلوب بالطريق المباشر، حيث تتولى المحكمة المختصة بالنزاع، توجيه الإنابة القضائية مباشرة إلى المحكمة الأجنبية المراد منها تنفيذ الإنابة القضائية، وذلك تطبيقا لمعاهدة دولية سابقة، أو وفقا لأحكام قانون الدولتين.

---

[1] سامح أحمد، المرجع السابق، ص505.

[2] أحمد عبد الحليم شاكر، المرجع السابق، ص156 وما بعدها.

تطرقت م26 من اتفاقية الرياض سالفة الذكر إلى طلب الإنابة القضائية وشروطه، كما تطرقت اتفاقيات لاهاي إلى طلب الإنابة، حيث نصت م4 من الاتفاقية الثالثة لعام 1970 على أن يكون طلب الإنابة القضائية بلغة الجهة المطلوب منها تنفيذها أو تصحب بترجمة لها.[1]
ويتضمن طلب الإنابة القضائية نوع القضية والجهة الصادر عنها الطلب، والجهة المطلوب منها التنفيذ، وكل البيانات التفصيلية المتعلقة بالقضية، وبالمهمة المطلوب القيام بها، وخاصة أسماء الشهود، ومحال إقاماتهم، ونوع الأسئلة المطلوب طرحها عليهم.

في م18 من اتفاقية الرياض سالفة الذكر تم بيان طريقة تنفيذ الإنابة القضائية، إذ تتم وفقا للإجراءات القانونية المعمول بها في قوانين الطرف المتعاقد المطلوب إليه ذلك، وفي حالة رغبة الطرف المتعاقد الطالب وبناء على طلب صريح منه...مع احترام كل الظروف التي تسمح للأطراف المعنية حضور التنفيذ.[2]

تطرقت م21 من إلى طلبات الإنابة القضائية في القضايا الجزائية، بحيث ينبغي أن ترسل الطلبات الخاصة بها عن طريق وزارة أو أمانة العدل لدى كل منها، وتنفذ بواسطة الجهات القضائية حسب إجراءات كل منها.

تجدر الإشارة أن الدول تستجيب لطلب إجراءات الإنابة القضائية حتى ولو لم تكن بينها اتفاقية، تطبيقا لمبدأ المجاملة الدولية، أو مبدأ المعاملة بالمثل؛ غير أن وجود اتفاقية خول الإنابة القضائية بين دولتين أو أكثر يدعم التعاون ويعززه، ويحدد أشكاله بأكثر دقة، مثل معاهدة الأمم المتحدة النموذجية لعام 1990، لتبادل المساعدة في المسائل الجنائية.

---

[1] المرجع نفسه، ص162.

[2] تنص م18 من اتفاقية الرياض العربية بشأن التعاون القضائي على ما يلي:
يتمّ تنفيذ الإنابة القضائية وفقاً للإجراءات القانونية المعمول بها في قوانين الطرف المتعاقد المطلوب إليه ذلك.
وفي حالة رغبة الطرف المتعاقد الطالب – بناءً على طلب صريح منه – في تنفيذ الإنابة القضائية وفق شكل خاص، يتعيّن على الطرف المتعاقد المطلوب إليه ذلك إجابة رغبته ما لم يتعارض ذلك مع قانونه أو أنظمته ويجب إذا أبدت الجهة الطالبة رغبتها صراحة – إخطارها في وقت مناسب بمكان وتاريخ تنفيذ الإنابة القضائية حتى يتسنى للأطراف المعنية أو وكلائهم حضور التنفيذ، وذلك وفقاً للحدود المسموح بها في قانون الطرف المتعاقد المطلوب إليه التنفيذ.

يكون للإجراء الذي يتم بطريق الإنابة القضائية الأثر القانوني نفسه كما لو كان تم أمام الجهة المختصة لدى الدولة طالبة الإنابة، وهذا ما نصت عليه صراحة م20 من اتفاقية الرياض سالفة الذكر.

لا يرتب تنفيذ الإنابة القضائية، الحقّ في اقتضاء أية رسوم أو مصروفات فيما عدا أتعاب الخبراء، إن كان لها مقتضى، ونفقات الشهود التي يلتزم الطالب بأدائها، ويرسل بها بيان مع ملف الإنابة، وللطرف المتعاقد المطلوب إليه تنفيذ الإنابة القضائية أن يتقاضى لحسابه ووفقاً لقوانينه الرسوم المقرّرة على الأوراق التي تقدّم أثناء تنفيذ الإنابة (م21 من اتفاقية الرياض سالفة الذكر).

الفرع الثالث: نقل الإجراءات الجزائية.

يعني نقل الإجراءات الجزائية أن تقوم إحدى الدول بنقل الإجراء الجزائي المنوط بها القيام به، إلى دولة أخرى بناء على طلبها، وتسمى هذه الأخيرة بالدولة المنقول إليها، وبناء أيضا على طلب المحكمة المختصة بنظر الدعوى، ويعتبر نقل الإجراءات الجزائية إحدى الآليات المتبعة كوسيلة لنقل الإجراءات بالتبادل تجاه الحالات التي يفشل فيها اتخاذ إجراءات تسليم المجرمين في الظروف المتشابهة، الأمر الذي يستوجب من الدولة المطلوب منها محاكمة المتهم، وبناء على ذلك تنقل إليها الإجراءات الجزائية إذا احتاجت إلى ذلك.

غالبا ما يتم نقل الإجراءات الجزائية من دولة إلى أخرى، عندما تكون هناك أكثر من دولة تقرر ولايتها واختصاصها في جريمة ما يتم التحقيق فيها.[1]

ومن شروط نقل الإجراءات الجزائية:

– أن يكون الفعل المنسوب ارتكابه إلى الشخص يشكل جريمة وفقا لقانون الدولتين طالبة نقل الإجراءات والمطلوب إليها، وهذا ما اشترطته م5/32 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات سالفة الذكر والتي لم تشترط أن تكيف الجريمة التكييف ذاته في البلدين، إذ يجوز أن تكيفها دولة على أنها جناية والدولة الأخرى تكيفها جنحة مثلا.

– أن تكون الإجراءات المطلوب اتخاذها مقررة في قانون الدولة المطلوب إليها عن الجريمة ذاتها.

[1] سامح أحمد، المرجع السابق، ص507.

– أن تكون الإجراءات المطلوب اتخاذها تؤدي إلى كشف الحقيقة، كأن تكون أدلة الجريمة موجودة بالدولة المطلوب إليها.

ولقد اهتم المجتمع الدولي بموضوع نقل الإجراءات الجزائية، فأبرمت معاهدات لها صلة بالموضوع، ومن أهمها معاهدة الأمم المتحدة النموذجية بشأن نقل الإجراءات في المسائل الجنائية، التي اعتمدت بقرار الجمعية العامة للأمم المتحدة رقم (118/45) الصادر في 1990/12/14.

كما أقر المجلس الأوربي اتفاقية نقل الإجراءات الجزائية، وهي تسمح للدول الأطراف بمحاكمة المتهمين طبقا لقوانينها، بناء على طلب دولة أخرى طرف في تلك الاتفاقية، شريطة أن يكون الفعل مجرما ومعاقبا عليه في كلتا الدولتين.[1]

ويحقق نقل الإجراءات الجزائية تقليص الآثار السلبية التي تنجم عن تنازع الاختصاص بين الدول، كما تفوت الفرصة على المجرمين الجاري التحقيق معهم في الإفلات من العقاب.

في القانون الفرنسي، وفي حالة الإنابة القضائية، يجوز لمأمور الضبط القضائي استدعاء الشهود، وعلى هؤلاء الحضور وتأدية واجب الشهادة طبقا لنص م113 ق إ ج ف، ويجوز للقاضي أن يحكم بالغرامة على من تخلف عن الحضور للشهادة طبقا لنص م109 ق إ ج ف.

رغم ذلك، يرى البعض أن هذه الاتفاقيات تمثل آليات تقليدية في مكافحة الجرائم ومعاقبة مرتكبيها، وهو ما قد لا يكون مجديا في إطار الجرائم الواقعة في البيئة الرقمية وخاصة الجرائم الواقعة على التجارة الإلكترونية، لما تسببه هذه الجرائم بسبب طبيعتها وسماتها ونوعية مرتكبيها، من صعاب جمة تتعلق بإقامة الدليل على ارتكابها، ومدى قبول التشريعات لدى مختلف الدول للأدلة المستمدة من الحاسب الآلي، وكذلك فيما يتعلق بالتحقيق والتفتيش والمعاينة والضبط...في الفضاء الرقمي، وتتبع المسارات الإلكترونية، كل هذه العوامل مجتمعة تؤدي في المحصلة إلى صعوبة بالغة في إثبات الجرائم الواقعة على التجارة الإلكترونية، ونسبتها إلى فاعليها، لذا دعت بعض التشريعات المقارنة إلى التعاون الدولي في مجال تفتيش النظم المعلوماتية، وغيرها من المسائل الفنية المتعلقة

[1] المرجع نفسه، ص508.

بالتقنيات الحديثة، مع الحرص على الحفاظ على سيادة الدول.[1] وهذا ما تفطن له منذ عام 1993 المجلس الأوربي حينما اقترح أن تمتد سلطة التفتيش إلى الأجهزة المعلوماتية المتواجدة بدائرة اختصاص جهة أجنبية بشرط وجود حالة الضرورة، وينبغي العمل على إيجاد سند قانوني لإجراء التفتيش الممتد خارج أقاليم الدول صونا لسيادتها، ولقد أرست الاتفاقية الأوربية حول الإجرام المعلوماتي لسنة 2001 قواعد المساعدة القضائية والتعاون القضائي، حينما تطرقت إلى إجراءات التسليم والمساعدة القضائية التي تأخذ بعين الاعتبار تجميع حركة البيانات في الزمن الفعلي، ومراقبة محتوى البيانات، وهو ما يجعل لجميع أطراف الاتفاقية الأوربية وجود نطاق مختلف تطبق فيه تلك الإجراءات.[2]

أما الاتفاقية العربية لمكافحة جرائم تقنية المعلومات فقد أكدت على أهمية التعاون بين الدول الأطراف، وتطرقت في الفصل الثالث من الاتفاقية إلى الأحكام الإجرائية من خلال نص المادة 22 وما بعدها، وقد نصت بعض المواد على التعاون بين الدول الأطراف من ذلك م32 الخاصة بالمساعدة المتبادلة وم33 الخاصة بالمعلومات العرضية المتلقاة، وم37 المتعلقة بالحفظ العاجل للمعلومات المخزنة، وم38 المتعلقة بالكشف العاجل عن معلومات محفوظة للمستخدمين، وم39 المتعلقة بالتعاون والمساعدة الثنائية المتعلقة بالوصول إلى معلومات تقنية المعلومات المخزنة، وم41 المتعلقة بالتعاون والمساعدة الثنائية بخصوص الجمع الفوري لمعلومات تتبع المستخدمين، وم42 والمتعلقة بالتعاون والمساعدة الثنائية فيما يخص المعلومات المتعلقة بالمحتوى.

الفرع الرابع: الاعتراف بتنفيذ الأحكام الجنائية.

تعتبر مرحلة تنفيذ الأحكام الجنائية من أهم مراحل التعاون الدولي في مجال مكافحة الجرائم بصفة عامة، حيث يتحول بموجبها منطوق الحكم من صيغته القانونية النظرية، إلى واقع ملموس، بحيث ينال المذنب جزاءه، ويأخذ المتضرر حقه.

والحكم الجنائي هو ذلك الحكم الصادر عن محكمة مختصة قانونا بالفصل في الدعوى الجزائية وفق القانون، والمكتسب للقوة التنفيذية.

[1] شيماء عبد الغني، المرجع السابق، ص274.

[2] سامح أحمد، المرجع السابق، ص509.

أما تنفيذ الحكم الأجنبي فهو إجراء قضائي، يمنح بموجبه الحكم الأجنبي الصيغة التنفيذية في الدولة، بحيث يصبح قابلا للتنفيذ.[1]

في فرنسا، فإن القاعدة العامة هناك هي أن القانون الجنائي الفرنسي لا يعترف بالقوة التنفيذية للحكم الجنائي الأجنبي؛ فعلى خلاف النصوص الصادرة في المواد المدنية والتجارية، لا يوجد نص في القانون الجنائي الفرنسي يسمح بإعطاء القوة التنفيذية لحكم جنائي أجنبي، وفي إيطاليا متى أصدر القاضي الإيطالي حكمه بتقرير نفاذ الحكم الأجنبي، يترتب على هذا الحكم أن تكون له القوة التنفيذية، ويثبت له أيضا حجية الشيء المقضي به، ولكي ينفذ الحكم الأجنبي في ألمانيا لا بد أن يتقرر بالأمر بالتنفيذ دون البحث في مشروعيته، وفي القانون الإنجليزي لا بد من رفع دعوى جديدة أمام القضاء الانجليزي تستند على الحكم الأجنبي، والأمر ذاته بالنسبة للدول الاسكندينافية.[2]

في اتفاقية الرياض العربية سالفة الذكر تطرقت م25/ب لتنفيذ الأحكام الأجنبية المدنية والتجارية دون الأحكام الجزائية. وهذا ما نلحظه أيضا من خلال نص م37 من اتفاقية التعاون القانوني والقضائي بين دول المغرب العربي سالفة الذكر.

هناك اتجاه دولي نحو الاعتراف بالحكم الأجنبي خاصة فيما يخص بعض الجرائم الخطيرة، – ونعتقد أن جرائم التجارة الإلكترونية من ضمن الجرائم الأكثر خطورة على المجتمع الدولي – والاتجاه نحو الاعتراف بالحكم الجنائي الأجنبي يمكن ملاحظته من خلال اتفاقية نقل السجناء المحكوم عليهم بعقوبات سالبة للحرية بين دول مجلس التعاون الخليجي، والذي يتيح للمحكوم عليه أو ذويه أو الجهات المختصة طلب تنفيذ العقوبات السالبة للحرية والصادرة من إحدى محاكم الدول الأعضاء في المجلس ضد مواطن خليجي من دولة أخرى غير الدولة التي صدر فيها الحكم، أن ينقل لتنفيذ العقوبة في موطن الجاني أو الدولة التي له فيها إقامة دائمة؛ ومراعاة للاعتبارات الإنسانية والعملية، وتفعيلا لمبدأ التعاون الدولي في تنفيذ الأحكام الجنائية الأجنبية.

---

[1] أحمد عبد النور، إشكالية تنفيذ الأحكام الأجنبية، مذكرة ماجستير في القانون الدولي الخاص، جامعة أبي بكر بلقايد، تلمسان2010/2009، ص2.

[2] متعب بن عبد الله السند، التعاون الدولي في تنفيذ الأحكام الجنائية وأثره في تحقيق العدالة، رسالة ماجستير في العدالة الجنائية، كلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية، الرياض 2011، ص72.

وهذا الاتجاه نحو الاعتراف بالحكم الجنائي الأجنبي يمكن ملاحظته على المستوى العربي كذلك، وإن اقتصر على بعض أنواع الجرائم الأكثر خطورة، ومن ذلك، مشروع الاتفاقية العربية لمكافحة الجريمة المنظمة عبر الحدود الوطنية، فقد جاء النص صراحة في المادة 38 على اعتراف الدول الأطراف في الاتفاقية بالأحكام الجنائية والمدنية الأجنبية النهائية الصادرة من محاكم الدول الأخرى الأطراف في الجرائم المشمولة بهذه الاتفاقية. باستثناء خمس حالات للأحكام المعترف بها وهي:

الأحكام المخالفة للشريعة الإسلامية.

-الأحكام المخالفة للأنظمة الأساسية.

-الأحكام المخالفة للدستور والنظام العام في الدولة المطلوب إليها الاعتراف.

-الأحكام التي ما زالت قابلة للطعن فيها بأحد أوجه الطعن المقررة في قانون الدولة التي صدر الحكم من إحدى محاكمها.

-الأحكام الصادرة في جريمة تدخل أصلا ضمن الولاية القضائية للدولة المطلوب منها أخذ الحكم في الاعتبار متى باشرت فيها أيّا من إجراءات التحقيق أو المحاكمة[1].

فيما يخص الجرائم الواقعة على التجارة الإلكترونية فإنها تواجه مشكلة الاعتراف بالحكم الأجنبي الصادر في جريمة منها بحق مجرم في دولة غير الدولة التي بها المحكمة مصدرة الحكم، وعليه فلا بد من التوسع في هذا النوع من الجرائم في عقد الاتفاقيات الدولية والإقليمية والثنائية فيما يخص تطبيق الأحكام الجنائية الأجنبية فيما بين الدول الأطراف، والاعتراف بهذه الأحكام وقوتها التنفيذية، وفق شروط وضوابط مسبقة ينص عليها في الاتفاقية، حتى تتدعم عملية التعاون الدولي في مجال مكافحة الجرائم الواقعة على التجارة الإلكترونية وتصبح أكثر فاعلية.

الجدير بالملاحظة أن الاتفاقية العربية لمكافحة جرائم تقنية المعلومات سالفة الذكر، لم تتطرق إلى موضوع تنفيذ الأحكام الجنائية الأجنبية رغم أهميته.[2]

---

[1] متعب بن عبد الله السند، المرجع السابق، ص75.

[2] يرى بعض الفقه أنه يجوز الرجوع إلى قواعد الإجراءات المدنية والإدارية، إذا أغفلت نصوص قانون الإجراءات الجزائية بعض الإجراءات أو عالجتها بشيء من النقص أو الغموض، شريطة أن تتضمن قواعد الإجراءات المدنية أحكاما عامة، يجوز الأخذ بها في النطاق الجزائي، لا مجرد أحكام استثنائية. يراجع: د. رؤوف عبيد، مبادئ الإجراءات الجنائية في القانون المصري، ط17، دار الجيل للطباعة، الفجالة، مصر 1989، ص15. وبناء على ما تقدم يجوز الأخذ بنص م605 من قانون الإجراءات المدنية والإدارية بالشروط الواردة في هذه المادة، فيما يخص تنفيذ الأحكام والقرارات الأجنبية المتعلقة بالجانب الجزائي. لكن رأيا فقهيا مخالفا يرى بأنه في حالة خلو قانون الإجراءات الجزائية من نص أو إحالة فإنه لا يجوز في هذه الحالة الرجوع

المطلب الثاني: تسليم المجرمين.

يعالج هذا المطلب من خلال التطرق إلى تعريف تسليم المجرمين وصور وشروط التسليم ا(لفرع الأول)، ثم إلى تسليم المجرمين في القانون الجزائري (الفرع الثاني).

الفرع الأول: تعريف تسليم المجرمين وصوره.

يعتبر تسليم المجرمين مجالا من مجالات التعاون القضائي الدولي، وقد تناولته بالتنظيم ترسانة كبيرة من القوانين الداخلية والاتفاقيات الدولية، كونه أكثر جوانب التعاون الدولي إثارة للجدل والمشكلات، بسبب ارتباطه المباشر بالحرية الشخصية، مما يستوجب الحرص الشديد والعناية الفائقة عند التعامل مع هذا الموضوع، درءا للأضرار التي قد تحيق بالأفراد إذا حدث تعسف في استخدامه، وموازنة المصلحة القانونية المتوخاة من ورائه ومصلحة الأشخاص في التمتع بكامل حقوقهم الشخصية، وعليه يجب أن يقدر التسليم بقدره، ويخضع بدقة للقواعد القانونية التي تنظمه.

يقوم التسليم على ساس العلاقات الدولية أيا كان نوع أو طبيعة الجريمة المرتكبة مما يدعم فكرة السيادة، ويحقق إجراء التسليم مصلحة المجتمع الدولي في عدم إتاحة الفرصة للمجرم من الإفلات من العقاب، وهو بذلك يحقق بالإضافة إلى الردع الخاص، الردع العام، ويمنع الغير من ارتكاب جرائمهم العابرة للحدود، كما أن مثول المتهم أمام قاضي موقع الجريمة يحقق أفضل الضمانات الخاصة بمحاكمة الشخص المطلوب، وإجراء التحقيقات بصورة أكثر فاعلية ونجاعة.[1]

إلى قانون الإجراءات المدنية والإدارية بحثا عن حل للمسألة، فكلا القانونين مستقل بذاته، لدرجة أنه لا يجوز اعتبار أحدهما فرعا للآخر، وإلا جاءت الحلول شاذة غير متوائمة. يراجع: د. محمد زكي أبو عامر، الإجراءات الجنائية، دار الجامعة الجديدة للنشر، الإسكندرية، مصر 2008، ص18. ولعل هذا هو الرأي الراجح، خاصة وأن المسألة هنا تتعلق بسيادة الدول، ناهيك عن أن المادة الأولى من قانون الإجراءات المدنية والإدارية قد نصت صراحة على تطبيق أحكام قانون الإجراءات المدنية والإدارية على الدعاوى المرفوعة أمام الجهات القضائية العادية والجهات القضائية الإدارية.

[1] طارق فوزي، المرجع السابق، ص265.

أولا: تعريف تسليم المجرمين.

تسليم المجرمين هو أن تسلم دولة (الدولة المطلوب منها التسليم) شخصا يوجد في إقليمها إلى دولة أخرى (الدولة الطالبة)، تبحث عن ذلك الشخص إما بهدف ملاحقته أو بهدف تسليط العقوبة التي حكمت بها عليه محاكمها.[1]

كما عرف تسليم المجرمين بأنه:"العملية الإجرائية الرسمية، التي تطلب بواسطتها إحدى الولايات القضائية، من ولاية قضائية أخرى إنفاذ إعادة شخص موجود في الولاية القضائية متلقية الطلب، متهم أو مدان بارتكاب جرم جنائي واحد أو أكثر، انتهاكا لقانون الولاية القضائية الطالبة. وتلتمس الإعادة لكي يواجه ذلك الشخص المحاكمة في الولاية القضائية الطالبة، أو لكي توقع عليه العقوبة على ذلك الجرم أو الجرائم".[2]

وعرف بعض الفقه تسليم المجرمين بأنه: "هو أن تسلم دولة شخصا موجودا في إقليمها إلى دولة أخرى بناء على طلبها، لتحاكمه عن جريمة يعاقب عليها قانونها، أو لتنفيذ فيه حكم صادر من محاكمها". وعليه فإن التسليم يشمل فئتين من الأشخاص: فئة المتهمين وفئة المحكوم عليهم، وقد استخدم المشرع اللبناني مصطلح "استرداد".[3]

يتميز التسليم عن الإبعاد بأن هذا الأخير قرار إداري، يضع حدا لإقامة أجنبي داخل البلاد،[4]كما يتميز التسليم عن المنع من دخول البلاد، حيث يعني هذا الأخير الحيلولة دون اجتياز شخص ما حدود الدولة، كما يتميز عن الإعادة إلى الوطن التي تعني إعادة بعض الأشخاص إلى أوطانهم من دون أن تطلبهم دولهم، وليس من الضروري أن يكونوا متهمين أو محكوم عليهم، فالإعادة تقع في سياق غير جنائي.[5]

---

[1] مكتب الأمم المتحدة المعني بالمخدرات والجريمة UNODC، دليل التعاون الدولي في المسائل الجنائية لمكافحة الإرهاب، مكتب الأمم المتحدة، فينا 2009، ص201.

[2] مكتب الأمم المتحدة المعني بالمخدرات والجريمة UNODC، دليل المساعدة القانونية المتبادلة وتسليم المجرمين، مكتب الأمم المتحدة، فينا 2013، ص41.

[3] ياسر محمد الجبور، تسليم المجرمين أو تقديمهم في الاتفاقيات الدولية والنظام الأساسي للمحكمة الجنائية الدولية، رسالة ماجستير في القانون العام، جامعة الشرق الأوسط، عمان، الأردن 2011، ص70.

[4] ياسر محمد الجبور، المرجع السابق، ص71.

[5] المرجع نفسه، ص72.

تطرقت م31 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات إلى موضوع تسليم المجرمين، من دون أن تتطرق إلى إعطاء تعريف سواء في هذه المادة، أو في الفصل الأول من الاتفاقية وخاصة م2 التي عنيت بتعريف بعض المصطلحات، ولعل ذلك راجع إلى أن موضوع تسليم المجرمين ليس حديثا، وهو متعلق بالجرائم الدولية والعالمية كلها، وليس مقصورا فقط على جرائم تقنية المعلومات.

ثانيا: صور وشروط تسليم المجرمين.

يرى الفقه المقارن أن تسليم المجرمين عمل إجرائي ذو طبيعة إدارية بالرغم من أنه يمر بمراحل قضائية تهدف إلى تسليم شخص لدولة أجنبية، لإجراء تحقيق مفتوح قبله، أو لإصدار حكم جنائي ضده، أو لتنفيذ هذا الحكم.

يقسم الفقه تسليم المجرمين إلى قسمين: تسليم إيجابي، وتسليم سلبي؛ فالتسليم السلبي هو الذي يتضمن ضمانات قضائية، ويتميز بالصبغة الإجرائية، وليس من الضروري في هذا النوع من التسليم أن يتم بناء على طلب دولة أجنبية، إذ يجوز تحريك إجراءاته بناء على رغبة الدولة التي يوجد بها المتهم أو المحكوم عليه، ويمر هذا النوع من التسليم بمرحلتين في الغالب، المرحلة الأولى قضائية والهدف منها حماية الحقوق الشخصية للمتهم أو المحكوم عليه، أما المرحلة الثانية فإدارية، وفيها تعمل الدولة على التعبير عن قرارها في شأن التسليم معتمدة على سيادتها، ومن الضروري أن تكون المرحلة القضائية للتسليم متعلقة بالفعل الذي من أجله كان طلب التسليم دون سواه، ولا أن يخضع المحكوم عليه أو المتهم لعقوبة تختلف عن تلك التي حكم بها أو يحكم بها بشأن التسليم؛ أما التسليم الإيجابي فهو أن تطلب دولة أجنبية تسليم المتهم أو المحكوم عليه، وهو ما يبدو في نظر غالب الفقه ذا طبيعة إدارية، إذ غالبا ما يطلب من وزارة العدل عن طريق السلك الدبلوماسي ووزارة الخارجية، كما نصت م8 من اتفاقية تسليم المجرمين بين دول الجامعة العربية الموقعة في 1953/06/09 على أن تقدم طلبات تسليم المجرمين وفقا لقوانين كل دولة،[1] وهذا ما أكدت عليه م5/31 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، سالفة الذكر إذ نصت بأن يخضع تسليم المجرمين للشروط المنصوص عليها في

[1] سامح أحمد، المرجع السابق، ص513.

قانون الدولة الطرف التي يقدم إليها الطلب أو لمعاهدات التسليم المطبقة بما في ذلك الأسس التي يجوز للدولة الطرف الاستناد عليها لرفض تسليم المجرمين.

يعتمد التسليم على المعاهدات المبرمة بين الدول من ذلك على سبيل المثال لا الحصر الاتفاقية المتعلقة بتنفيذ الأحكام وتسليم المجرمين المبرمة بين الجزائر وفرنسا[1] واتفاقية الرياض العربية سالفة الذكر في المادة 38 وما بعدها، والاتفاقية العربية لمكافحة جرائم تقنية المعلومات سالفة الذكر، وهذه الاتفاقيات قد تكون ثنائية، أو تكون متعددة الأطراف، وقد تكون اتفاقيات التسليم دولية تتضمن أحكاما متعلقة بتنظيم تسليم المجرمين دون أن تكون بحد ذاتها اتفاقية تسليم، وعند انعدام المعاهدات بين الدول أو انعدام التشريع الداخلي المنظم لمسألة التسليم، لا حل أمام الدول سوى القبول بنظام التسليم طبقا لما استقر عليه العرف الدولي في هذا الصدد، مع اشتراط المعاملة بالمثل، وقد تقبل بعض الدول ذلك دون هذا الشرط، لعدة أسباب معظمها سياسية.[2]

يجب التحقق من استيفاء شروط التسليم، وتختلف هذه الأخيرة باختلاف ما تتضمنه الاتفاقيات الدولية، سواء ما تعلق منها بتسليم المجرمين، أو بمكافحة نوع معين من الجرائم، غير أن هناك ضوابط عامة لتسليم المجرمين تتبعها غالبية الاتفاقيات والمعاهدات، من أبرزها أن يشكل الفعل جريمة من الجرائم الجائز بشأنها التسليم، وهنا تختلف الاتفاقيات فيما بينها وتنقسم إلى نهجين رئيسيين؛ الأول يقوم على التعداد الحصري للجرائم التي يجوز فيها التسليم، أما النهج الثاني فيعتمد على وضع قائمة للجرائم أو الأحوال التي لا يجوز فيها التسليم، وكلا النهجين يعتمد مبدأ ازدواج التجريم، بمعنى أن يكون الفعل مجرما في كلا الدولتين، طالبة التسليم والمطلوب منها كقاعدة عامة، وهناك نهج جسامة الجريمة أو الحد الأدنى من العقوبة، وهناك النهج المختلط.

ويعد النهج الأول الأقل شيوعا لأنه يؤدي إلى إفلات بعض المجرمين من العقاب متى كانت الجريمة غير واردة في القائمة، رغم ذلك نجد الاتفاقية العربية لمكافحة جرائم تقنية المعلومات سالفة الذكر قد أخذت بالنهج الأول حينما ذكرت م1/31 منها بأن تسليم المجرمين ينطبق على الجرائم المنصوص عليها في الفصل الثاني من الاتفاقية بشرط أن تكون تلك الجرائم يعاقب عليها في قوانين الدول الأطراف المعنية بسلب الحرية لفترة أدناها سنة واحدة أو بعقوبة أشد؛ والجرائم المذكورة

[1] الأمر رقم 194/65 المؤرخ في 29 يوليو 1965، ج ر68، الصادرة سنة 1965، ص962.

[2] سامح أحمد، المرجع السابق، ص514.

في الفصل الثاني هي جريمة الدخول غير المشروع (م6)، جريمة الاعتراض غير المشروع (م7)، الاعتداء على سلامة البيانات (م8)، جريمة إساءة استخدام وسائل تقنية المعلومات (م9)، جريمة التزوير (م10)، جريمة الاحتيال (م11)، جريمة الإباحية والجرائم المرتبطة بها (م12، م13)، جريمة الاعتداء على حرمة الحياة الخاصة (م14)، الجرائم المتعلقة بالإرهاب والمرتكبة بواسطة تقنية المعلومات (م15)، الجرائم المتعلقة بالجرائم المنظمة والمرتكبة بواسطة تقنية المعلومات (م16)، الجرائم المتعلقة بانتهاك حقوق المؤلف والحقوق المجاورة (م17)، الاستخدام غير المشروع لأدوات الدفع الإلكترونية (م18).

الملاحظ أن م1/31 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات قد حذت حذو الاتفاقية الأوربية للإجرام المعلوماتي لسنة 2001، حيث نصت م24 منها على تطبيق هذه المادة على عملية تسليم المجرمين فيما بين الدول الأطراف بالنسبة للجرائم المنصوص عليها وفقا للمواد من 2-11 الواردة في الاتفاقية، بشرط أن يعاقب عليها القانون ...بالحرمان من الحرية لفترة سنة واحدة على الأقل أو بعقوبة أشد، والأمر نفسه قد نصت عليه اتفاقية الرياض العربية للتعاون القضائي التي دخلت حيز النفاذ ابتداء من 1985/10/30، في م40/أ تحت مسمى الأشخاص الواجب تسليمهم.

غير أن النهج الثاني القائم على استبعاد بعض الجرائم أو الأحوال من نطاق مبدأ تسليم المجرمين هو الأكثر شيوعا في الاتفاقيات الدولية.

تستبعد أيضا من نطاق التسليم الجرائم السياسية، ولعل الأمر راجع إلى أن السياسي يجب معاملته معاملة خاصة، لأنه غالبا ما يحمل على عاتقه هموم مجتمعه، ولأن بعض الأنظمة لما يتكرس فيها النظام الديمقراطي، وقد خلت معظم الاتفاقيات الدولية والقوانين الوطنية من تعريف الجريمة السياسية، بيد أنه تم استبعاد أفعال عديدة من دائرة الجرائم السياسية، فلا يجوز بأي حال من الأحوال اعتبار الاغتيالات وجرائم القتل الأخرى، والتسبب في إحداث عاهات للغير، والاختطاف وأعمال العنف وجرائم الإرهاب، من قبيل الجرائم السياسية، وهذا ما أشارت إليه م41 من اتفاقية الرياض العربية للتعاون القضائي سالفة الذكر في إحدى فقراتها: "وفي تطبيق أحكام هذه الاتفاقية لا تعتبر من الجرائم ذات الصبغة السياسية المشار إليها في الفقرة (أ) من هذه المادة ولو كانت بهدف سياسي الجرائم الآتية:

– التعدّي على ملوك ورؤساء الأطراف المتعاقدة أو زوجاتهم أو أصولهم أو فروعهم.

– التعدّي على أولياء العهد أو نواب الرؤساء لدى الأطراف المتعاقدة.
– القتل العمد والسرقة المصحوبة بإكراه ضد الأفراد السلطات أو وسائل النقل والمواصلات".

ويجد الاتجاه الداعي إلى عدم جواز التسليم في الجرائم السياسية تطبيقا له في م3/أ من معاهدة الأمم المتحدة النموذجية بشأن تسليم المجرمين لعام 1990، وفي م1/3 من الاتفاقية الأوربية لعام 1957، وفي م4 من اتفاقية تسليم المجرمين لدول الجامعة العربية عام 1952، وفي م6/أ من الاتفاقية العربية لمكافحة الإرهاب لعام 1998،[1] وم41/أ من اتفاقية الرياض العربية للتعاون القضائي سالفة الذكر، كما أن م1/35 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات أجازت للدولة الطرف المطلوب منها المساعدة أن ترفض الطلب إذا كان قانونها الداخلي يعتبر الجريمة من الجرائم السياسية.

تستبعد أيضا الجرائم العسكرية من نطاق تسليم المجرمين، حيث تحرص العديد من الدول على استبعاد هذا النوع من الجرائم من نطاق التسليم لارتباطه بمؤسسة حساسة من مؤسسات الدولة، وهي المؤسسة العسكرية، لذا نجد الكثير من الاتفاقيات قد نصت على حظر التسليم بالنسبة لهذه الجرائم، ومنها الاتفاقية الأوربية لعام 1957، وم6/ب من الاتفاقية العربية لمكافحة الإرهاب، وم41/ب من اتفاقية الرياض العربية للتعاون القضائي سالفة الذكر.

كما لا يجوز التسليم بالنسبة للجرائم قليلة الأهمية، والتي ليست على قدر من الخطورة، ولا تتلاءم مع النفقات التي تتطلبها إجراءات التسليم.

كما لا يجوز التسليم بالنسبة للجرائم المحكوم فيها على المتهم المطلوب تسليمه بعقوبة الإعدام، وهذا الأمر بالنسبة للدول التي ألغت عقوبة الإعدام في قوانينها الداخلية، وتعتبرها هدرا لحقوق الإنسان ومساسا بأقدس حق له وهو الحق في الحياة، وهو ما يشكل بعض المشاكل في بعض الأحيان، إذا كانت الدولة الطالبة تجيز عقوبة الإعدام، وقد نصت م4/د من معاهدة الأمم المتحدة النموذجية لسنة 1990 سالفة الذكر على جواز التسليم في هذه الحالة، بشرط أن تقدم الدولة طالبة التسليم ضمانات تكفل عدم تنفيذ عقوبة الإعدام في شأن الشخص المطلوب تسليمه.

[1] سامح أحمد، المرجع السابق، ص516.

كما أن بعض الدول تحظر تسليم مواطنيها لدول أخرى، وقد يجد هذا الأمر سنده في دساتير هذه الدول، ولعل ذلك راجع إلى عدم رغبة هذه الدول في أن يتابع مواطنوها من قبل قضاء أجنبي لأنها قد تعتبر ذلك نوعا من الإهانة لها والتعدي على سيادتها، وعلى النقيض من ذلك لا تجد بعض الدول غضاضة في أن تسمح بتسليم مواطنيها في إطار من التعاون القضائي في مجال القبض على الهاربين وإعادتهم، ذلك أن تحقيق العدالة مطلب الجميع وينبغي تضافر الجهود للوصول إليه، ويستوي في ذلك أن يكون المجرم من مواطنيها أم لا، وقد حاولت الاتفاقيات أن تجد حلا وسطا للمسألة، بعدم إلزام الدولة تسليم مواطنيها، مع ضرورة أن تتم متابعتهم، من ذلك ما نصت عليه م39 من اتفاقية الرياض العربية سالفة الذكر: " يجوز لكل طرف من الأطراف المتعاقدة أن يمتنع عن تسليم مواطنيه ويتعهّد في الحدود التي يمتدّ إليها اختصاصه، بتوجيه الاتهام ضد من يرتكب منهم لدى أي من الأطراف المتعاقدة الأخرى جرائم معاقباً عليها في قانون كل من الدولتين بعقوبة سالبة للحرية مدّتها سنة أو بعقوبة أشدّ لدى أي من الطرفين المتعاقدين وذلك إذا ما وجه إليه الطرف المتعاقد الآخر طلباً بالملاحقة مصحوباً بالملفات والوثائق والأشياء والمعلومات التي تكون في حيازته ويحيط الطرف المتعاقد الطالب علماً بما تمّ في شأن طلبه.
وتحدّد الجنسية في تاريخ وقوع الجريمة المطلوب من أجلها التسليم".

الأمر ذاته نصت عليه م6/ح من الاتفاقية العربية لمكافحة الإرهاب، والأمر نفسه نجده في م10/16 من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية لسنة 2000،كما نصت م4/أ من معاهدة الأمم المتحدة النموذجية لتسليم المجرمين على رفض التسليم إذا كان الشخص المراد تسليمه من رعايا الدولة المطالَبة، ولم تشذ الاتفاقية العربية لمكافحة جرائم تقنية المعلومات عن هذه القاعدة، حيث نصت م6/31 منها على:"يجوز لكل دولة طرف من الأطراف المتعاقدة أن تمتنع عن تسليم مواطنيها، وتتعهد في الحدود التي يمتد إليها اختصاصها، بتوجيه الاتهام ضد من يرتكب منهم لدى أي من الدول الأطراف الأخرى جرائم معاقبا عليها في قانون كل من الدولتين بعقوبة سالبة للحرية مدتها سنة، أو بعقوبة أشد لدى أي من الطرفين المتعاقدين، وذلك إذا ما وجهت إليها الدولة الطرف الأخرى طلبا بالملاحقة، مصحوبا بالملفات والوثائق والأشياء والمعلومات التي تكون في حيازتها، وتحاط الدولة الطرف الطالبة علما بما يتم في شأن طلبها، وتحدد الجنسية في تاريخ وقوع الجريمة المطلوب من أجلها التسليم".

كما لا يجوز حسب القواعد العامة محاكمة الشخص عن الجريمة ذاتها مرتين، مما يؤدي إلى عدم جواز تسليمه من أجل محاكمته عن الجريمة ذاتها، وهذا ما نصت عليه مثلا م41/د من اتفاقية الرياض العربية للتعاون القضائي سالفة الذكر: "لا يجوز التسليم إذا كانت الجريمة قد صدر بشأنها حكم نهائي (مكتسب الدرجة القطعية) لدى الطرف المتعاقد المطلوب إليه التسليم".

كما يحظر تسليم ممنوحي حق اللجوء السياسي.[1]

وعادة فإن رفض تسليم المتهمين أو المحكوم عليهم، غالبا ما يكون عائقا من معوقات التعاون القضائي، وهو ما يؤثر على الجرائم الإلكترونية بصفة عامة، لذا دعت الاتفاقية الأوربية حول الإجرام المعلوماتي لسنة 2001، في م3/24 إلى الاعتماد على هذه الاتفاقية كأساس لتوقيف الشخص المطلوب تسليمه، إذا كان رفض التسليم راجعا إلى عدم وجود اتفاقية تسليم مع الطرف طالب التسليم، وأن المعاهدة المبرمة لا تشمل هذا الطلب، الأمر ذاته تبنته الاتفاقية العربية لمكافحة جرائم تقنية المعلومات في نص م3/31: "إذا قامت دولة ما بجعل تسليم المجرمين مشروطا بوجود معاهدة، وقامت باستلام طلب لتسليم المجرمين من دولة طرف أخرى ليس لديها معاهدة تسليم فيمكن (يجوز) اعتبار هذه الاتفاقية كأساس قانوني لتسليم المجرمين فيما يتعلق بالجرائم المذكورة في الفقرة (1) من هذه المادة".

يمر تسليم المجرمين المعلوم تواجدهم بعدة مراحل تتبعها الدول، وتلتزم باحترام عدد من الإجراءات سبق تحديدها بموجب الاتفاقية، أو وفقا لما جرى عليه العرف الدولي في حالة عدم وجود اتفاقية.

نصت م9/16 من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة لعام 2000 على:"يجوز للدولة الطرف متلقية الطلب رهنا بأحكام قانونها الداخلي، وما ترتبط به من معاهدات لتسليم المجرمين، وبناء على طلب الدولة الطرف الطالبة، أن تحتجز الشخص المراد تسليمه والموجود في إقليمها، أو أن تتخذ تدابير مناسبة أخرى لضمان حضوره إجراءات التسليم، متى اقتنعت بأن الظروف تسوغ ذلك، وبأنها ظروف ملحة"، الأمر ذاته تقريبا قررته م24 من الاتفاقية العربية لمكافحة الإرهاب لعام 1998 سالفة الذكر، أما م42 من اتفاقية الرياض العربية للتعاون القضائي سالفة الذكر

[1] سامح أحمد، المرجع السابق، ص519.

فقد نصت على:" يقدّم طلب التسليم كتابة من الجهة المختصة لدى الطرف المتعاقد طالب التسليم إلى الجهة المختصة لدى الطرف المتعاقد المطلوب إليه التسليم ويجب أن يرفق الطلب بما يأتي.

أ. بيان مفصّل عن هوية الشخص المطلوب تسليمه وأوصافه وجنسيته وصورته إن أمكن.

ب. أمر القبض على الشخص المطلوب تسليمه أو أية وثيقة أخرى لها نفس القوة صادرة من الجهات المختصّة أو أصل حكم الإدانة الصادر طبقاً للأوضاع المقرّرة في قانون الطرف المتعاقد الطالب أو صورة رسمية له مصدّقاً عليها من الجهة المختصة لدى الطرف المتعاقد الطالب.

ج. مذكرة تتضمن تاريخ ومكان ارتكاب الأفعال المطلوب التسليم من أجلها وتكييفها والمقتضيات الشرعية أو القانونية المطّبقة عليها مع نسخة معتمدة من هذه المقتضيات وبيان من سلطة التحقيق بالأدلة القائمة ضد الشخص المطلوب تسليمه".

تتم دراسة ملف التسليم من قبل سلطة الادعاء العام أو النيابة العامة في الدولة المطلوب منها التسليم، للتأكد من موافقة طلب التسليم للشروط المطلوبة بهذا الصدد، وتقدير مدى صحة أدلة إثبات التهمة بحق الشخص المطلوب تسليمه، وتختلف السلطة المختصة بالفصل في طلب التسليم والبت فيه من دولة إلى أخرى، ففي انجلترا وفرنسا وإيطاليا تفصل في الطلب السلطة القضائية، أما في مصر وإسبانيا والبرتغال فتفصل فيه السلطة التنفيذية ويخضع الفصل في طلب التسليم بالقبول أو الرفض لرقابة القضاء الإداري في الدولة المطلوب إليها التسليم.[1]

في حالة تعدد طلبات التسليم، بحيث تتقدم العديد من الدول بطلباتها بشأن تسليم متهم أو محكوم عليه، فإن الأولوية في التسليم تكون للدولة التي تضررت من الجريمة، ثم للدولة التي ارتكبت الجريمة على ترابها، ثم للدولة التي ينتمي إليها المطلوب تسليمه، حسب نص م46 من اتفاقية الرياض العربية سالفة الذكر وم13 من اتفاقية تسليم المجرمين بين جامعة الدول العربية لعام 1953، وإذا كانت طلبات التسليم عن جرائم مختلفة ارتكبها الشخص المطلوب تسليمه، تكون الأولوية للدولة التي طلبت التسليم قبل غيرها.

[1] سامح أحمد، المرجع السابق، ص521.

الفرع الثاني: تسليم المجرمين في القانون الجزائري

إن القواعد العامة بشأن التسليم المتعلقة بمختلف الجرائم، يجوز إعمالها بالنسبة للتسليم في الجرائم الإلكترونية، وفق ما ورد من نصوص في قانون الإجراءات الجزائية من المواد 694 إلى 720.

هذه المواد عالجت في الفصل الأول شروط تسليم المجرمين (المواد 694- 701 ق ا ج)، وفي الفصل الثاني إجراءات التسليم (م702-م713)، وفي الفصل الثالث آثار التسليم (م714-م718)، وفي الفصل الرابع موضوع العبور (م719 – 720 ق ا ج).

من استقراء هذه النصوص القانونية، نجد المشرع الجزائري قد نص على شروط التسليم وهي: أن يكون هناك تجريم مزدوج (م2/697 ق ا ج)، عدم جواز تسليم المتمتعين بالجنسية الجزائرية (م698 ق ا ج)، عدم جواز تسليم من تمت محاكمتهم عن الجريمة ذاتها المطلوب التسليم لأجلها (م4/698 ق ا ج).

المطلب الثالث: التعاون الدولي الأمني في مكافحة الجرائم الواقعة على التجارة الإلكترونية.

يعالج هذا المطلب من خلال التطرق إلى تعريف التعاون الدولي الأمني (الفرع الأول)، والجهود الدولية التي تبذلها مختلف الأطراف المعنية للتصدي للجرائم بصفة عامة، والجرائم المعلوماتية بصفة خاصة (الفرع الثاني)، ثم التعاون الدولي في مجال التدريب على مواجهة الجرائم الإلكترونية (الفرع الثالث).

الفرع الأول: تعريف التعاون الدولي الأمني.

تحتاج الدول، من أجل العيش بسلام مع غيرها من الدول إلى قدر من الأمن والنظام، ومن الأمور التي تؤرق بال الدول وتهدد أمنها واستقرارها الجرائم عبر الوطنية، وأبرزها الجرائم الإلكترونية، ولقد أثبت الواقع العملي أن أي دولة مهما كانت قوتها لا تستطيع وحدها القضاء على الجريمة، خاصة مع التطور المذهل في كافة مناحي الحياة؛ فنتيجة التطور الفائق في الاتصالات وتكنولوجيا المعلومات، وظهور الانترنت وانتشارها السريع ظهرت أشكال وأنماط جديدة من الجرائم هي الجرائم المعلوماتية أو الإلكترونية، باتت تشكل خطرا محدقا ليس على سرية النظم الحاسوبية أو

سلامتها أو توافرها فحسب، وإنما أيضا على البنى الأساسية الحرجة،[1] ومع تميز هذه الجرائم – بسبب طبيعتها – بالعالمية، فإن مكافحتها لا تؤتي ثمارها إلا بوجود تعاون دولي، بحيث يسمح بالاتصال المباشر بين أجهزة شرطة الدول المختلفة، وذلك بإنشاء مكاتب متخصصة لجمع المعلومات عن الجرائم الإلكترونية وتعميمها.[2]

التعاون الدولي الأمني بمفهومه الواسع يشمل مجالات مختلفة، كالمجال الشرطي، والمجال القانوني والمجال القضائي، لأن تحقيق الأمن والاستقرار يتطلب تضافر الجهود في هذه المجالات كلها، مع العناية بحقوق المتهمين والضحايا، ومراعاة سيادة الدول.

يعرف التعاون الدولي الأمني بأنه: "تبادل العون والمساعدة وتضافر الجهود المشتركة بين طرفين دوليين أو أكثر، لتحقيق نفع أو خدمة أو مصلحة مشتركة، في مجال التصدي لمخاطر الإجرام وما يرتبط به من مجالات أخرى، مثل مجال العدالة الجنائية ومجال الأمن، أو لتخطي مشكلة الحدود والسيادة التي قد تعترض الجهود الوطنية لملاحقة المجرمين وتعقب مصادر التهديد، سواء كانت المساعدة المتبادلة قانونية أو قضائية أو شرطية، وسواء اقتصرت على دولتين فقط أو امتدت إقليميا أو عالميا".[3]

التعاون الأمني على الصعيد الدولي ينبغي أن يرمي إلى منع ارتكاب الجرائم، عن طريق العمل على كشفها في مهدها، أي في مراحلها التحضيرية، من خلال تطوير آليات البحث والتنقيب والتحري بما فيها الآليات المستحدثة بفضل التكنولوجيا الحديثة؛ فإذا كانت الجرائم المعلوماتية ترتكب بوسائل تقنية فيجب التصدي لها بالوسائل ذاتها، وهو ما يتطلب تحسين القدرات البشرية والتقنية للأجهزة الأمنية المعنية بمكافحة هذا النوع من الجرائم.

نظرا لما تتسم به الجرائم المتعلقة بالمعلوماتية بصفة عامة، فإن مكافحتها الأمنية يجب أن ترتكز على الأسس التالية:[4]

---

[1] الغافري، المرجع السابق، ص636.

[2] المرجع نفسه، ص637.

[3] القريوي، المرجع السابق، ص38.

[4] سامح أحمد، المرجع السابق، ص524-525.

– التناول العلمي لبحث ظاهرة الجرائم الإلكترونية عامة والجرائم الواقعة على التجارة الإلكترونية بصفة خاصة، وتوفير المعلومات الإحصائية والبيانات اللازمة، سواء ما تعلق منها بالجريمة نفسها أو ما تعلق بمرتكبيها، أو بسير نظام القضاء الجزائي، إذ تساعد هذه المعلومات على التعامل مع هذا النوع من الجرائم بصورة فعالة ومناسبة، ولذا يجب إنشاء مركز دولي للمعلومات والبيانات الخاصة بتلك الجرائم على مختلف صورها، بما في ذلك أسماء المتورطين في الجرائم والإجراءات المتخذة بشأنهم، والتحقيقات التي جرت معهم...بمعنى عام وضع قاعدة بيانات دولية تشمل الجرائم والمجرمين وكل من له صلة بهم يمكن الرجوع إليها في أي وقت من قبل الدول الأعضاء حتى يسهل عليها وضع سياسات أمنية وتشريعية واتخاذ التدابير الملائمة في سبيل منع انتشار تلك الجرائم، أو الحد من آثارها والوقاية منها.

– التنسيق بين المؤسسات الأمنية بآلياتها المختلفة على الأصعدة الأمنية الإقليمية والدولية، بما يحقق تضييق الخناق على المجرمين وحصر نطاق جرائمهم، والحيلولة دون انتشارها، واستكمال أي نقص في المعلومات الأمنية، عن طريق التعاون المشترك لتجميع عناصر تلك المعلومات، وإتاحة الفرصة للتدارس والمناقشة حول الثغرات الأمنية الدولية، والعمل على سدها، وإيجاد أفضل أساليب التصدي للجريمة، وإتاحة الفرصة للتعرف على تجارب الدول الأمنية في هذا المجال، وخاصة تلك التي حققت نتائج طيبة، ولها خبرات في مجال مكافحة الجرائم المعلوماتية.

– تحديد سبل التعاون في مجال التدريب، والتعاون التقني، وضرورة تحقيق التكامل الأمني بين مختلف الأجهزة الأمنية المختصة للدول.

– إعداد مدونة دولية تتضمن توحيد المعايير والأركان القانونية التي تقوم عليها هذه الجرائم، ونطاق الأفعال المجرمة فيها.

– وضع استراتيجيات وقائية قادرة على تهيئة المناخ الملائم لأعمال مجابهة الجرائم، وتضييق الخناق على أنشطة المنظمات الإجرامية، وحرمانها من البيئة الملائمة لممارسة أنشطتها الإجرامية، وزيادة الوعي العام لدى فئات المجتمع، بنشر كافة المعلومات عن طبيعة هذه الجرائم وأساليب مرتكبيها.

– القيام ببعض العمليات الشرطية والأمنية المشتركة تدعيما للتعاون وصقلا للمهارات.

الفرع الثاني: الجهود الدولية في مجال التعاون الأمني.

إن مكافحة الجريمة مهمة جميع الأجهزة الدولية، ولقد ظهرت هذه المسألة على الصعيد الدولي نتيجة لتطور سبل الاتصالات والمواصلات واختصار المسافات، إذ غدا العالم قرية واحدة، وبذلك أضحى المجتمع الدولي بأسره يواجه التهديدات ذاتها في الكثير من القضايا، ولو بدرجات متفاوتة، لذلك كان من مصلحة الجميع إرساء سبل التعاون، من ذلك محاولة منع الجريمة قبل ارتكابها، وهو عمل بوليسي يقع على عاتق أجهزة الشرطة؛ وبقدر كفاءة الشرطة في تحقيق منع الجريمة يقاس أمن الوطن، وتتخذ أجهزة الشرطة التدابير والاحتياطات اللازمة لتحقيق ذلك، كذلك ضرورة الوقاية من الجرائم عن طريق التصدي للأسباب الجوهرية المسؤولة عن السلوك الإجرامي، وهنا يلعب علماء الإجرام وعلماء النفس وعلماء المجتمع وغيرهم دورا رئيسا في تقديم الحلول الجوهرية لمثل هذه المشاكل وكيفية التعامل معها، خاصة وأن الجرائم المعلوماتية جرائم من نوع خاص يقوم بها مجرمون يختلفون تماما عن المجرمين التقليديين، وعليه يجب استخدام عناصر التقدم العلمي والتقني للوقاية من الجرائم المعلوماتية.

لقد بذلت جهود دولية معتبرة لمواجهة الجرائم المعلوماتية من ذلك ما قامت به الأمم المتحدة عبر هيئاتها المختصة بمكافحة الجريمة، ومن أهم جهودها في هذا الميدان عقد عديد المؤتمرات بهذا الشأن، كما أنشئ عام 1997 مركز لمنع الجريمة الدولية بفينا، بهدف مكافحة الجرائم المنظمة عبر الوطنية، ومنها الجرائم الإلكترونية، كما عقدت العديد من الاتفاقيات والمعاهدات سواء المتعلقة بتسليم المجرمين أو بالجريمة المنظمة أو بالفساد...

ولعل من أبرز آليات التعاون الأمني على المستوى الدولي الجهود التي تقوم بها المنظمة الدولية للشرطة الجنائية "الانتربول"، وكذا بعض المنظمات الأخرى.

أولا: جهود المنظمة الدولية للشرطة الجنائية.

تعرف المنظمة الدولية للشرطة الجنائية اختصارا ب: "Interpol" والتي تعني: "Criminal Police International Organization" بالانجليزية، وينحصر الغرض من هذه المنظمة حسب نص م2 من ميثاقها كالآتي:

– تأكيد المعونة المتبادلة وتشجيعها في أوسع نطاق ممكن من سلطات الشرطة الجنائية، وفي حدود القوانين القائمة في الدول المختلفة، وفي نطاق الإعلان العالمي لحقوق الإنسان.
– أن تسهم بدور فعال في منع جرائم القانون العام ومكافحتها، وذلك بإقامة النظم التي تساعد على ذلك.

ترجع البدايات الأولى للتعاون الدولي الشرطي إلى سنة 1904، عندما تم إبرام الاتفاقية الدولية الخاصة بمكافحة الرقيق الأبيض، والتي نصت في مادتها الأولى على تعيين سلطة لجمع المعلومات الخاصة بموضوع الاتفاقية، لها الحق في مخاطبة بصفة مباشرة الإدارة المماثلة لها في كل الدول الأطراف المتعاقدة، ولم تمر سنة واحدة على إبرام هذه الاتفاقية إلا وكانت سبع دول من الدول المتعاقدة قد أنشأت مثل تلك الأجهزة لتتبادل من خلالها المعلومات والبيانات المتعلقة بموضوع الاتفاقية بغية القضاء على هذه الجريمة في أقاليمها.[1]

بعد ذلك أخذ التعاون الشرطي الدولي يأخذ صورة المؤتمرات الدولية، أولها مؤتمر موناكو عام 1914، والذي ضم رجال الشرطة والقضاء والقانون من أربع عشرة دولة لمناقشة بعض المسائل الشرطية، منها مدى إمكانية إنشاء مكتب دولي للتسجيل الجنائي، وتنسيق إجراءات تسليم المجرمين، إلا أن هذا الحلم قد تبخر نتيجة قيام الحرب العالمية الأولى. وبعد أن وضعت الحرب الكونية الأولى أوزارها حاول الكولونيل الهولندي "فان هوتين" عام 1919 إحياء فكرة التعاون الدولي الشرطي غير أنه لم يوفق في مسعاه.[2]

ومع نهاية عام 1923 نجح مدير شرطة فينا "جوهانو سويرا" في عقد ثاني مؤتمر دولي للشرطة الجنائية، ضم مندوبي تسع عشرة دولة، كان من نتائجه ولادة "اللجنة الدولية للشرطة الجنائية" المعروفة اختصارا ب: "ICPO" يكون مقرها "فينا"، وتعمل على التنسيق بين أجهزة الشرطة من أجل التعاون في مكافحة الجريمة.[3]

[1] الغافري، المرجع السابق، ص638.
[2] المرجع نفسه، ص638.
[3] المرجع نفسه، ص639.

غير أن اندلاع الحرب الكونية الثانية جعل اللجنة توقف نشاطها إلى غاية عام 1946، حيث عقد بالعاصمة البلجيكية بروكسل مؤتمر دولي يهدف إلى بعث مبادئ التعاون الأمني من جديد ووضعها موضع التنفيذ، وأسفر المؤتمر عن إحياء اللجنة الدولية للشرطة الجنائية، ونقل مقرها إلى العاصمة الفرنسية باريس، وغُير اسمها ليصير المنظمة الدولية للشرطة الجنائية،[1] وتم تشكيل لجنة تنفيذية من خمسة أعضاء برئاسة المفتش العام للسلطة البلجيكية، وفي سنة 1989 أصبح مقر المنظمة الجديد رسميا في مدينة "ليون" الفرنسية، وبلغ سنة 1998 عدد أعضائها إلى 177 دولة، وهو في تزايد مستمر.[2]

ومن الأمثلة على دور "الانتربول" فيما يتعلق بالجرائم المعلوماتية ما حصل في لبنان، عندما تم توقيف طالب جامعي من قبل القضاء اللبناني بتهمة إرسال صور إباحية لقاصرة من موقعه على شبكة الانترنت، إثر تلقي النيابة العامة اللبنانية برقية من الانتربول في ألمانيا بهذا الخصوص.[3]

وتصدر الانتربول نشراتها باللغات الرسمية الأربع وهي العربية والفرنسية والانجليزية والاسبانية، وهي حاليا ستة أنواع من النشرات؛ نشرة حمراء لطلب توقيف المطلوبين بغية تسليمهم، نشرة صفراء لتحديد مكان وجود المفقودين، نشرة زرقاء لتحديد مكان إقامة الأشخاص وجمع معلومات بخصوصهم، نشرة سوداء لتبين الجثث المجهولة، ونشرة برتقالية لإعطاء إشعارات تحذيرية عن تهديدات إرهابية محتملة. وتشمل نشاطات الانتربول ذات الأولوية مجالات الأمن العام، وجرائم الإرهاب والمنظمات الإجرامية، والجرائم المتعلقة بالمخدرات، والإجرام المالي، وجرائم التكنولوجيا المتقدمة كجرائم تقنية المعلومات، وجرائم الاتجار بالبشر، وإسناد التحقيق بشأن المجرمين الفارين.[4]

نظمت الأمانة العامة للانتربول أول مؤتمراتها الدولية عام 1994 بخصوص الغش والاحتيال، فيما يتعلق ببطاقات الائتمان التي تعتبر أهم وسائل الدفع بالنسبة للتجارة الإلكترونية، وخرجت بتوصيتين هما:

---

[1] المرجع نفسه، ص639.

[2] السقا، المرجع السابق، ص504.

[3] الغافري، المرجع السابق، ص640.

[4] سامح أحمد، المرجع السابق، ص530.

– ضرورة مراجعة الدول الأعضاء لتشريعاتها وقوانينها المتعلقة ببطاقة الائتمان، بما يضمن تجريم تصنيع أو امتلاك البطاقات المزورة، أو امتلاك معلومات غير قانونية، أو تم الحصول عليها بطريقة غير مشروعة، واستخدامها في إدخالها نظام بطاقات الائتمان.

– إنشاء مجموعات عمل شرطية من خبراء في الاحتيال الدولي التابعين لشرطة "هونغ كونغ" والشرطة الكندية، والخدمة السرية الأمريكية، وخدمة الاستخبارات الوطنية الجنائية لزيلاندا الجديدة، ومندوبين من منظمات بطاقات الائتمان؛ لمكافحة هذا النوع من الجرائم، والتقوا جميعهم في شهر فبراير 1995، وتم وضع الأسس الخاصة بتبادل المعلومات بهدف الحد من هذه الجرائم.

وقد قامت منظمة الانتربول بتوقيع خمس اتفاقيات مع المنظمات الراعية للبطاقات، وهي "أمريكان إكسبريس"، و"ديسكفري"، و"إيروباي انترناشيونال"، و"ماستر كارد الدولية"، وا"لفيزا الدولية"، من أجل مزيد من التعاون في مجال جرائم بطاقات الائتمان.[1]

وبوسع الانتربول تنسيق الموارد الميدانية في التحقيقات الجارية في مجال تكنولوجيا المعلومات بالتعاون مع الدول الأعضاء، ومن بين أمثلة التعاون طلب دولة كولومبيا في مارس 2008 من الانتربول إجراء فحوص أدلة جنائية مستقلة على أجهزة ومعدات حاسبات آلية، تم ضبطها خلال عملية لمكافحة المخدرات، نفذت ضد معسكر للقوات المسلحة الثورية الكولمبية (الفارك)، لتحديد ما إذا كان قد جرى التلاعب بمضمون أي من المعدات أو المستندات أو المحررات المخزنة على الحاسب الآلي لوزارة الدفاع، وما إذا كان قد تم المساس بحجيتها الإلكترونية، وبعد إجراء فريق من خبراء الانتربول لدراسة فنية أكد غياب أي دليل يشير إلى تعديل ملفات المستخدمين أو تحريفها، أو الإضافة عليها.[2]

أنشأت الانتربول خلال عام 2004 وحدة خاصة لمكافحة جرائم التكنولوجيا، كما قامت المنظمة بالتعاون مع مجموعة الدول الثمانية الكبرى G8 بوضع استراتيجيات لمواجهة هذا النوع من الجرائم من خلال:[3]

---

[1] السقا، المرجع السابق، ص508.

[2] أيمن رمضان، المرجع السابق، ص423.

[3] سامح أحمد، المرجع السابق، ص535.

– إنشاء مركز اتصالات أمني عبر الشبكة يعمل دون توقف، على مستوى مصالح الشرطة في الدول الأطراف.

– استخدام وسائل حديثة في المكافحة كاستخدام قاعدة البيانات المركزية للصور الإباحية المحولة من قبل الدول الأطراف والتي تستخدم برنامج (Excalibur) للتحليل والمقارنة الأوتوماتيكية لتلك الصور.

– تزويد شرطة الدول الأطراف بكتيبات إرشادية حول الجرائم الإلكترونية وكيفية التدريب على مكافحتها والتحقيق فيها، من مثل الكتيب المسمى "دليل جرائم الحاسب الآلي".

من الوقائع العملية التي تم الاستعانة فيها بالانتربول لمواجهتها في إطار جرائم الانترنت، العملية التي قامت بها المباحث الفدرالية الأمريكية بالتعاون مع الانتربول، والخاصة بتعقب الشخص الذي قام بنشر فيروس "دودة الحب" عبر شبكة الانترنت في الفليبين.

ثانيا:جهود جهاز الشرطة الأوربية.

جهاز الشرطة الأوربية أو "اليوروبول"، يعبر عن تجسيد طموحات الدول الأوربية في إنشاء جهاز يقوم بمساعدة السلطات الوطنية المكلفة بالمتابعة القضائية والأمن، من أجل التنسيق في مجال التحقيقات والتحريات، وإنشاء بنك معلومات للتقييم والاستغلال المركزي، ورسم استراتيجيات العمل على المستوى الأوربي، وتم توقيع معاهدة إنشاء "اليوروبول" في 1995/07/23، وتتلخص مهامه في تحسين سبل التعاون الشرطي بين الدول الأعضاء في الاتحاد، ومكافحة كل الأشكال الخطيرة للإجرام الدولي، عن طريق مد المحققين بمساعداته التقنية.[1]

ومن التطبيقات العملية للتعاون الدولي في الجرائم الإلكترونية ما سمي ب: "عملية أوديسيوس" التي تمت في 2004/02/26 بمبادرة من "اليوروبول"، وقامت قوات الشرطة خلالها بعمليات شملت عشر دول.[2]

[1] مختار شبيلي، المرجع السابق، ص123.

[2] هذه الدول هي: أستراليا، بلجيكا، كندا، ألمانيا، هولندا، النرويج، بيرو، إسبانيا، السويد، وبريطانيا.

من التطبيقات العملية للتعاون الدولي ما سمي "عملية محطم الجليد"، التي قامت بها اليوروبول في 2005/06/14 حيث تم خلالها مداهمة وتفتيش شبكات الحاسب الآلي في ثلاث عشرة دولة أوربية،[1] وتم توقيف أفراد في بعض من هذه الدول.[2]

ثالثا: دور اليوروجست في الكشف عن الجرائم الإلكترونية.

يساعد جهاز اليوروجست "EUROJUST" على التعاون القضائي والشرطي في مجال مكافحة الجرائم ومن بينها الجرائم الإلكترونية كما تنص على ذلك م4 من قرار مجلس الاتحاد الأوربي، وينعقد اختصاصه حينما يمس الإجرام دولتين على الأقل من أعضاء الاتحاد الأوربي، أو دولة عضو مع دولة من دول العالم الثالث، أو دولة عضو مع الرابطة الأوربية، وعمله بذلك لا يقتصر على الأفراد، بل يمتد إلى المؤسسات، وينسق جهاز اليوروجست مع اليوروبول إذ يزوده بالتحليلات اللازمة للقيام بالتحقيقات في الجرائم المنظمة.[3]

رابعا: المدعي العام الأوربي:

يعتبر منصب المدعي العام الأوربي منصبا مستقلا، أنشئ بغية حماية المصالح المالية للمجموعة الأوربية.

يقوم المدعي العام الأوربي بتحريك الدعوى العمومية أمام الهيئات القضائية المختصة في الدول الأعضاء، ويراقب أنشطة البحث والتحري في دول الاتحاد.

يحدد مجلس الاتحاد شروط مباشرة المدعي العام لمهامه، وهي ذات علاقة بمختلف الجرائم المرتبطة بحماية المصالح المالية للاتحاد كجرائم الغش والفساد وتبييض الأموال، وتزوير بطاقات الائتمان، وما ينتج عن ذلك من عقوبات عن هذه الجرائم.

كما يؤدي مجلس الاتحاد دورا رقابيا على أعمال المدعي العام في نطاق تنفيذ مهامه.[4]

---

[1] هذه الدول هي: النمسا، بلجيكا، فرنسا، ألمانيا، المجر، أيسلندا، إيطاليا، هولندا، بولندا، البرتغال، سلوفاكيا، السويد، وبريطانيا.

[2] أيمن رمضان، المرجع السابق، ص424.

[3] أيمن رمضان، المرجع السابق، ص425، ويراجع أيضا: مختار شبيلي، المرجع السابق، ص121.

[4] مختار شبيلي، المرجع السابق، ص122.

خامسا: دور مجلس وزراء الداخلية العرب.

ظهرت فكرة إنشاء مجلس وزراء الداخلية العرب سنة 1977 في المؤتمر الأول لاجتماع وزراء الداخلية العرب بالعاصمة المصرية، وتبلورت هذه الفكرة في المؤتمر الثالث لهؤلاء الوزراء بمدينة الطائف السعودية عام 1980، وعُقد مؤتمر استثنائي للوزراء العرب بالرياض عام 1982 لوضع مشروع النظام الأساسي للمجلس، وفي ديسمبر 1982 أقر مجلس جامعة الدول العربية نظام مجلس وزراء الداخلية العرب، وحل هذا النظام محل المنظمة السابقة المسماة "منظمة الدفاع الاجتماعي ضد الجريمة" وأصبح المجلس يمارس الاختصاصات المتعلقة بالأمن ومكافحة الجريمة على مستوى الدول العربية.[1]

سادسا: دور المنظمة الدولية لضباط الجرائم المالية.

تعرف هذه المنظمة اختصارا ب: "IAFCI"[2]وهي منظمة دولية غير ربحية، تم إنشاؤها عام 1986 عن طريق التعاون بين 68 محققا دوليا مختصا في جرائم الأموال، وتم من خلالها إنشاء منظمة دولية لضباط جرائم بطاقات الائتمان. وتتيح عضوية هذه المنظمة لأعضائها الحصول على المعلومات السرية الخاصة بالجرائم المالية الدولية، وبالمجرمين الدوليين، وتبعث تحذيرات لأعضائها بالأماكن المعرضة لهذه الجرائم، كما تسمح للعضو الدخول على شبكات الحاسب الآلي التي تخص الجرائم المالية.[3]

سابعا: التعاون من خلال نظام "شنجين" للمعلومات.

يتكون نظام معلومات "شنجين" من قسم مركزي مقره مدينة "ستراسبورغ" الفرنسية، وأقسام وطنية في كل دولة من دول المنظمة، وما يميزه هو بنك المعلومات الكبير الذي تسجل فيه المعلومات التي ترسلها إليه قوات الشرطة والسلطات القضائية في كل دولة، ومن بين هذه المعلومات عناوينُ الأفراد سواء أولئك المطلوب تسليمهم من قبل دول أخرى، أو الممنوعين من دخول أراضي

[1] السقا، المرجع السابق، ص509.

[2] International Association Of Financial Crimes Investigators.

[3] السقا، المرجع السابق، ص511.

دولة ما عضو، أو المعلن اختفاؤهم، أو المطلوب تقديمهم للعدالة بأمر قضائي لأي سبب من الأسباب.[1]

الفرع الثالث: التعاون الدولي في مجال التدريب على مواجهة الجرائم الإلكترونية.

إن التقدم المتواصل في تكنولوجيا الحاسب الآلي والإنترنت يفرض على الجهات المسؤولة في الدولة، أن تسير بخطوات متناسقة مع التطورات السريعة التي تشهدها هذه التقنيات، والإلمام بها حتى يمكن التصدي للأفعال الإجرامية التي صاحبت هذه التكنولوجيا ومواجهتها، هذا من ناحية، ومن ناحية أخرى فإن إعمال القانون في مواجهة الجرائم المعلوماتية يستلزم اتخاذ إجراءات قد تتجاوز المفاهيم والمبادئ المستقرة في القوانين العقابية التقليدية، لما تتسم به هذه الجرائم من حداثة في الأسلوب وسرعة في التنفيذ وسهولة في إخفائها والقدرة على محو آثارها؛ حيث أثبتت الوقائع العملية أن هناك جرائم متعلقة بالحاسب الآلي وشبكة الإنترنت قد ارتكبت على مرأى ومسمع من رجال الشرطة، بل قام بعض رجال الشرطة بتقديم يد المساعدة لمرتكبي هذه الجرائم دون قصد وعن جهل، أو على سبيل واجبات المهنة التي يلزمهم بها هذا القانون، مثلما حدث عندما طلبت إحدى دوائر الشرطة بالولايات المتحدة الأمريكية من شركة تعرضت للقرصنة أن تتوقف عن تشغيل جهازها الآلي لتتمكن من وضعه تحت المراقبة بهدف كشف مرتكب الجريمة، ونتيجة لذلك أتلف ما كان قد سلم من الملفات والبرامج، وإتلاف الأدلة قد يقع كذلك عن خطأ مشترك بين الخبراء وبين الجهة المجني عليها، فمثلا في تحقيق إحدى الجرائم المعلوماتية والتي تدور وقائعها حول طلب أحد الأشخاص من إحدى الشركات زعم أنه وضع قنبلة معلوماتية بنظام حاسبها الآلي، تبين أن الشركة وقبل إبلاغ السلطات المختصة كانت قد استدعت خبيرا للتحقق من صحة ذلك وإبطال مفعول القنبلة إن وجدت، وبالفعل نجح الخبير في اكتشاف القنبلة وإزالتها من البرنامج الموضوعة فيه، وعندما تولت الشرطة التحقيق اتضح أنه بإزالة القنبلة أتلفت كل الأدلة على وجودها؛[2] وبالتالي فإن ظهور هذه الأنماط الجديدة من الجرائم أصبح يشكل عبئاً ثقيلا على عاتق جميع أجهزة العدالة الجنائية سواء رجال الضبط القضائي أو رجال التحقيق أو المحاكم على مختلف درجاتها، خصوصا وأن متطلبات العدالة، تقتضي أن تتحمل الأجهزة الأمنية الحكومية كامل المسؤولية تجاه اكتشاف كافة الجرائم

[1] أيمن رمضان، المرجع السابق، ص426.

[2] الغافري، المرجع السابق، ص676.

المعلوماتية وضبط الجناة فيها وتحقيق العدالة في حقهم، لأجل ذلك كان لا بد أن تكون تلك الأجهزة على مختلف أنواعها على درجة كبيرة من الكفاءة والمعرفة والقدرة على كشف غموض تلك الجرائم والتعرف على مرتكبيها بسرعة ودقة متناهيين، ولا يتأتى هذا الأمر إلا بالتدريب الجيد،[1] فكفاءة رجال العدالة لمواجهة هذه الظواهر المستحدثة وقدرتهم في التصدي لها لا بد وأن ترتكز على كيفية تطوير العملية التدريبية،[2] والارتقاء بها والنهوض بأساليب تحقيقها لأهدافها. من هذا المنطلق كانت الدعوة إلى وجوب تأهيل القائمين على هذه الأجهزة[3]، وضرورة وجود تعاون دولي في مجال تدريب رجال العدالة.

أولا: التدريب وأهميته في مجال مكافحة الجرائم الإلكترونية.

التدريب يعد جزءا من عملية التنمية الإدارية وهو يهتم بالدرجة الأولى بالكفاءة والفعالية في إنجاز العمل، من هنا فقد حرصت الكثير من المنظمات العامة والخاصة على العناية به، باعتباره أحد الأدوات الأساسية لرفع مستوى الأداء وزيادة الكفاءة الإنتاجية وإعداد العاملين على اختلاف مستوياتهم للقيام بواجبات أعمالهم والمهام الموكلة إليهم على خير وجه، إضافة إلى تهيئتهم لتحمل المزيد من المسؤوليات من خلال زيادة قدراتهم على مواجهة المهام المعقدة في الحاضر والمستقبل، ولهذا أصبح ينظر إلى التدريب على أنه وسيلة للاستثمار الذي تلجأ إليه المنظمات الإدارية لتحقيق أهدافها باعتباره عنصرا حيويا لا بد منه لبناء الخبرات والمهارات المتجددة .

وقد أصبح التدريب يلعب دورا هاما في حياة الإنسان في عصرنا الحاضر، ويمكن القول بأننا نعيش اليوم عصر التدريب، فقد زاد الاهتمام بمختلف جوانبه الفنية والتكتيكية فقد أضحى ضرورة للفرد المتدرب وللمنظمة التي ينتسب إليها في آن واحد، سواء أكانت منظمة مدنية أم عسكرية، حكومية أم خاصة، تعمل في قطاع العدالة أم في غيره، فهو أحد العناصر الأساسية لزيادة

---

[1] د. هشام فريد محمد رستم : الجرائم المعلوماتية ، مرجع سابق ص 439-440.

[2] يعرف التدريب بأنه: نشاط مستمر ومخطط يهدف إلى سد الفجوة بين الأداء الحالي والأداء المتوقع لشاغل الوظيفة فهو يقوم على أساس تحديد المهارات والقدرات الواجب توافرها في شاغل الوظيفة، ومن ثم إحداث التغييرات في سلوك وقدرات الفرد أو الجماعة المسئولة عن أداء هذه الوظيفة" يراجع: صالح محمد النويجم : تقويم كفاءة العملية التدريبية في معاهد التدريب الأمنية بمدينة الرياض من وجهة نظر العاملين فيها، رسالة ماجستير في العلوم الإدارية ، جامعة نايف العربية للعلوم الأمنية الرياض 2005م ص 9.

[3] وتعرف العملية التدريبية بأنها " مجموع الأنشطة أو العمليات الفرعية التي توجه لعدد من المتدربين لتحقيق أهداف معينة في برنامج تدريبي معين وتحدث الأثر أو الآثار المطلوبة فيه" أنظر، صالح محمد النويجم: المرجع السابق ص 7.

كفاءة العنصر البشري ورفع إنتاجيته وتحقيق التنمية بمفهومها الشامل.

والهدف من عملية التدريب إدخال وإحداث تعديلات جوهرية على سلوك المتدربين، تبدو آثارها واضحة في سلوكهم لأداء الأعمال التي يكفلون بها على أحسن وجه، كل في مجال تخصصه، وبشكل أفضل بعد عملية التدريب لا قبلها.[1]

وتبدوا أهمية التدريب وضرورته في أنه من ناحية يعد الوسيلة الفعلية والتطبيقية الناجحة والمؤثرة التي تكفل الاستفادة من مهارات وتجارب الآخرين، من خلال أشخاص أكفاء مؤهلين وقادرين على نقل هذه التجارب وتلك المهارات بوسائل سهلة بسيطة، كما أنه يعد من ناحية أخرى الوسيلة الملائمة والفعالة لوضع المعارف العلمية موضع التطبيق الفعلي والتعرف على الأخطاء والسلبيات التي يمكن أن يكشف عنها التطبيق العملي، ووضع الحلول الكفيلة بتجنبها، وتزداد أهمية التدريب في الوقت الحاضر نظرا للتطور التكنولوجي الكبير الذي يشهده العالم اليوم.[2]

والتدريب المقصود هنا ليس التدريب التقليدي فحسب فلا يكفي أن تتوافر لدى رجال العدالة الجزائية الخلفية القانونية أو أركان العمل الشرطي، وإنما لا بد من إكسابهم خبرة فنية في مجال الجريمة الإلكترونية، وهذه الخبرة الفنية لا تتأتى دون تدريب تخصصي تراعى فيه العناصر الشخصية للمتدرب من حيث توافر الصلاحية العلمية والقدرات الذهنية والنفسية لتلقي التدريب، وتثبت التجارب على الأرض، أنه من الأيسر تدريب متخصص في تكنولوجيا المعلومات وشبكات الاتصال بدلا من تدريب القائمين على تنفيذ القانون كرجال الشرطة أو ممثلي الإدعاء العام، ويذهب بعض الخبراء إلى أنه يجب أن تتوافر لدى المتدرب خبرة لا تقل عن خمس سنوات في المجالات ذات العلاقة بتكنولوجيا المعلومات كالبرمجة وتصميم النظم وتحليلها وإدارة الشبكات وعمليات الحاسب الآلي[3].

وبالنسبة للمنهج التدريبي فيجب أن يشتمل على بيان بالمخاطر والتهديدات ونقاط الضعف وأماكن الاختراقات لشبكة المعلومات وأجهزة الحاسب الآلي مع ذكر لمفاهيم معالجة البيانات وتحديد نوعية و أنماط الجرائم المعلوماتية، وبيان لأهم الصفات التي يتميز بها المجرم المعلوماتي، والدوافع

[1] صالح محمد النويجم، المرجع السابق ص 1.

[2] د. محمد السيد عرفة، تدريب رجال العدالة وأثره في تحقيق العدالة، جامعة نايف العربية للعلوم الأمنية ، الرياض 2005 ص 2.

[3] د. هشام محمد فريد رستم – الجرائم المعلوماتية " أصول التحقيق الجنائي الفني " – بحث مقدم لمؤتمر القانون والكمبيوتر والإنترنت –كلية الشريعة والقانون بجامعة الإمارات العربية المتحدة في الفترة 1-2000/5/3م المجلد الثاني– الطبعة الثالثة – 2004 م ص 496.

وراء ارتكاب الجرائم المعلوماتية.

وفيما يتعلق بمنهج التحقيق فإنه لا بد وأن يشتمل على[1]: 1. إجراءات التحقيق، 2.التخطيط للتحقيق، 3.تجميع المعلومات وتحليلها، 4.أساليب المواجهة والاستجواب، 5.مراجعة النظم الفنية للبيانات، 6. أساليب المعمل الجنائي.

بالإضافة إلى ذلك لا بد وأن يشتمل على ما يتعلق بالتفتيش والضبط وكيفية استخدام الحاسب الآلي كأداة للمراجعة والحصول على أدلة الاتهام وما يخص الملاحقة الدولية والتعاون المشترك.

وفيما يخص التدريب فإنه لا بد وأن يراعى في البرنامج التدريبي نوعه وصفته وما إذا كان رسميا من خلال حلقات دراسية أو حلقات نقاش – ورش العمل- حول هذا النوع المستحدث من الجرائم، وحلقات النقاش التي يمكن أن تثمر أفضل تدريب رسمي هي تلك التي تكفل تفاعل المشاركين، وتتضمن تحليلا لحالات دراسية وإكساب خبرة عملية في كيفية التعامل مع الحاسب الآلي وكيفية استخدام تقنيات الاتصال بين شبكات الحاسب الآلي، وما يرتبط بها من قواعد بيانات ومعلومات. وقد يكون البرنامج التدريبي غير رسمي من خلال تكليف المتدرب بالعمل مع شخص لديه خبرة في تحقيق الجرائم المعلوماتية، أو التدريب باستخدام أسلوب الفريق والذي تقوم فلسفته على تدريب الفريق أو مجموعة متخصصة في جرائم الحاسب الآلي مرة واحدة بحيث يكون لكل فريق من الفرق مهمة محددة فضلا عن إلمامه بمهام زملائه الآخرين، فطبقا لهذا الأسلوب يتم التركيز على تدريب مجموعة من المتخصصين في مجالات معينة بحيث يلم كل منهم بتخصص الآخرين، ويزداد في الوقت نفسه فهما لتخصصه الأصلي[2].

ويتعين هنا على الفريق أن يخوض تجارب عملية بحيث تعرض عليه عينة من الجرائم المعلوماتية التي تم التحقيق فيها، على أن يراعى في هذه العينة التنويع لكي تؤدي دورها في إكساب

---

[1] المرجع نفسه، ص 497.

[2] يمكن تقسيم الفريق إلى ثلاث مجموعات رئيسة هي:

المجموعة الأولي: مهمتها تنفيذ القانون.

المجموعة الثانية: مهمتها التدقيق والمراجعة الحسابية.

المجموعة الثالثة: مهمتها معالجة البيانات إلكترونيا.

يراجع: الغامدي، المرجع السابق، ص681.

المشاركين في البرنامج التدريبي الخبرة المطلوبة، وهذا الأمر يتطلب أن يعهد بالتدريب إلى جهات متخصصة تعنى باختيار المدربين ممن تتوافر لديهم الصلاحية العلمية والفنية والصفات الشخصية ليتولوا التدريب في هذا المجال، والذي من شأنه تحقيق نتائج طيبة في عملية التدريب[1]. والعلمية التدريبية لا بد وأن تكون مستمرة ولا تتوقف عند حد معين، سيما وأن الجرائم المعلوماتية ومنها الجرائم المتعلقة بالتجارة الإلكترونية في تطور مستمر وبشكل سريع جدا.

ليس هذا فحسب بل لا بد وأن تسعى الأجهزة الأمنية المعنية بالتحقيق إلى استقطاب المتخصصين والكفاءات في المجال المعلوماتي وضمهم إليها ليكونوا ضمن إطاراتها والاستفادة منهم، ومن أجل ذلك ينبغي على كليات الشرطة من جهة أن تعمل جاهدة لقبول دفعات من الجامعين من خريجي كليات الحاسبات الآلية لتخرجهم ضباطاً مؤهلين قانونيا وتقنيا، كذلك يتعين على الكليات المعينة بتدريس القانون أن تسعى جاهدة إلى تدريس الحاسبات الآلية وكل ما يتعلق به إلى الطلبة، وأن تكون مادة الحاسب الآلي وتقنية المعلومات إحدى المواد الأساسية، لأن من شأن ذلك أن تتكون لدي خريجي هذه الكليات ثقافة قانونية وثقافة حاسوبية.

صفوة القول وخلاصته أن غرس و تطوير الثقافة الحاسوبية وسط رجال القانون والشرطة، وربطها بالثقافة القانونية والشرطية التقليدية يكفل للأجهزة الأمنية ولسلطات التحقيق النجاح الباهر في مواجهة الجرائم المعلوماتية.

ثانيا: مظاهر التعاون الدولي في مجال تدريب رجال العدالة الجزائية.

أجهزة العدالة في الكثير من الدول، خاصة دول العالم الثالث ليست لديها تلك الجاهزية لمواجهة الجرائم المتعلقة بالتجارة الإلكترونية ومثيلاتها من الجرائم المستحدثة ذات التطور المستمر، لعدة أسباب منها، الافتقار إلى الموارد الكافية مادية كانت أو بشرية، أو لأن سلطات

[1] من الأمثلة على أنماط التدريب والاهتمام به على المستوى العالمي:

في الولايات المتحدة الأمريكية التدريب على تحقيق الجرائم المعلوماتية يتم من خلال دورات متخصصة مدة كل دورة أربعة أسابيع ويتم ذلك بمعرفة أكاديمية مكتب التحقيقات الفيدرالي الأمريكي في كوانتيكو Quantico وفيرجينيا. Virginia

في كندا تنظم الشرطة الملكية الكندية دورات متخصصة مدة كل دورة 4 أسابيع يتم فيها التدرب على تقنيات وأساليب تحقيق الجريمة المعلوماتية وذلك بكلية الشرطة في مدينة أوتاوي .وتشتمل موضوعات من خمسة مواضيع هي :1.أساسيات الحاسبات والمعالجة الإلكترونية للبيانات 2. مقدمة في برمجة الحاسوب3.أمن الحاسبات وشبكات المعلومات4.القانون والإثبات5.الجريمة المعلوماتية. الغافري، المرجع السابق، ص682.

التحقيق لديها محدودة أو لأنه لديها قوانين ونظم سبقها الزمن أو قد تفتقر لأي قوانين لتتصدى بها لهذه النوعية من الجرائم.

بما أنه ما من دولة يمكنها النجاح في مواجهة هذه الأنماط المستحدثة بمفردها دون تعاون وتنسيق مع غيرها من الدول، كانت الدعوة إلى ضرورة وجود تعاون دولي، ليس فقط في مجال المساعدات القضائية المتبادلة أو في مجال تسليم المجرمين فحسب، وإنما أيضا في مجال تدريب رجال العدالة[1]، فتدريب الإطارات البشرية القائمة على إنفاذ القانون ليس بالمستوى نفسه في جميع الدول، بل يتفاوت من دولة لأخرى بحسب تقدم الدولة ورقيها، أو ضعفها وتخلفها، وعند إمعان النظر في بعض الاتفاقيات الدولية والإقليمية، نجدها تدعو وبصريح النص إلى ضرورة وجود تعاون بين الدول في مجال التدريب ونقل الخبرات فيما بينها. كما هو الحال في المادة 29 من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية 2000.

والتعاون الدولي في مجال تدريب رجال العدالة على مواجهة الجرائم الواقعة على التجارة الإلكترونية قد يكون بين الدول وأجهزة العدالة الجزائية لديها، فعلى الصعيد العربي نجد مثلا أنه هناك اجتماعات تم عقدها في إطار التنسيق بين المعاهد القضائية العربية لتوفير التدريب والتأهيل المناسبين لأعضاء الهيئات القضائية العربية. وقد تمخضت الاجتماعات عن الاتفاق على إعداد مشروع اتفاقية للتعاون بين المعاهد القضائية العربية تسمي اتفاقية عمّان للتعاون العلمي بين المعاهد القضائية العربية والتي وقعت في 9 إبريل 1997م [2]، وفي دول عربية كثيرة نجد أن النيابة العامة تعقد الكثير من الندوات والمؤتمرات وحلقات النقاش وتشارك فيها، بالإضافة أنه يتم إرسال أعضاء النيابة من مختلف الدرجات في برامج خارجية وذلك بالتعاون مع أجهزة النيابة العامة في الدول الأخرى والهيئات الدولية بهدف الإطلاع على أحدث النظم المقارنة، وقد يتم من خلال عقد ندوات ومؤتمرات أو ورشات

[1] يقصد بتدريب رجال العدالة تلك العملية التي يخطط لها وتصمم لها البرامج ، ويبذل الجهد والمال لتغير سلوك العاملين في أجهزة العدالة ، سواء أكانوا من القضاء أو من رجال التحقيق والادعاء العام " النيابة العامة " أو من رجال الضبط الجنائي ، أو من رجال السلطة العامة القائمين على تنفيذ القانون أو من الموظفين المعاونين لهذه الأجهزة كالخبراء وغيرهم ، أو من المهنيين الذين يشاركون في تحقيق العدالة كالمحامين، حيث تهدف هذه العملية إلى تغير سلوكهم ورفع مستوى مهارتهم واتجاهاتهم، بما يكفل حسن إنجاز العمل القانوني والقضائي والتنفيذي، مما ينعكس إيجابا على الارتقاء بكيفية أداء العدالة وتقديمها للمتقاضين بشكل يكفل إقامة التوازن بين المصلحة العامة من جهة والمصلحة الخاصة للأفراد من ناحية أخرى ، مما يجعل الناس يطمئنون إلى جدية وفاعلية سير العدالة ، فيبعث ذلك على الثقة وتحقيق الأمن للجميع. محمد سيد عرفة : المرجع السابق ص 9.

[2] الغافري، المرجع السابق، ص684.

العمل الجماعي المتخصصة في مواجهة تلك الجرائم، التي تعقد على المستوى الدولي أو على المستوى الإقليمي، حيث تلقي هذه الفعاليات العلمية من أبحاثها ودراستها وموضوعات محاورها الضوء على المستجدات المتعلقة بالجرائم المستحدثة من خلال تحليل ومناقشة أبعادها بعقلية ناجحة مما يمكن المعنيين بالوقاية ومكافحة هذه الجرائم من التعرف على أساليب ارتكابها وأخطارها ووسائل الوقاية والمكافحة بأساليب تتناسب وتفوق أساليب ووسائل مرتكبيها. وعلى هامش هذه المؤتمرات أو الندوات أو ورشات العمل الجماعي تعقد اللقاءات وتبادل الآراء والخبرات.[1]

وقد يتحقق من عقد اللقاءات وحلقات المناقشة المصغرة بين مسؤولي الاتصال بالسفارات أو المكاتب الجغرافية الإقليمية للمنظمات والأجهزة المعنية مع جهات أو أطراف يقعون في دائرة عملهم أو بالقرب منها بناء على رغبة الجهة التي يمثلونها، يتم خلالها تبادل الآراء والخبرات بين المشاركين. وتمثل كافة هذه اللقاءات وحلقات المناقشة وسيلة طيبة للحوار والمناقشة والتشاور للتعارف وتبادل الرأي والخبرة وطرح الأفكار والتصورات وتدارس سبل تنمية وتشجيع التعاون فيما بين الأطراف.

وقد يتحقق عن طريق تنظيم الدورات التدريبية للعاملين في أجهزة العدالة الجزائية والمعنيين بمكافحة الجريمة على المستوى الدولي، وتعد هذه الصورة أكثر تطورا للتعاون الدولي الذي يستهدف تقريب وجهات النظر وتوحيد المفاهيم بين المشاركين في مكافحة الجريمة في الدول المختلفة من خلال تبادل الخبرة، وطرح موضوعات ومشكلات للتدارس المشترك، والتعرف على أحدث التطورات في مجال الجريمة سيما المعلوماتية وأساليب مكافحتها، وغالبا ما يجري تنظيم مثل هذا التدريب من خلال المنظمات أو الدول أو الأجهزة الكبرى ذات مستوى أكثر تقدما يمكن أن يشجع الأطراف الأخرى على المشاركة في هذه البرامج التدريبية، كما يمكنها تحمل نفقات وأعباء مثل هذه الدورات، وتحقق مثل هذه الدورات والبرامج العديد من الفوائد للجهات المنظمة وللمشاركين فيها، فالجهة المنظمة يمكنها من خلال عقد مثل هذه البرامج أن تطرح ما تريد من موضوعات حيوية، كما أنها تعلن عن دورها الرائد لتزيد من ثقة الأطراف الأخرى في أدائها، بما يشجع على إجراء المزيد من التعاون معها، وبما يضعها في مكانه خاصة لدى المتدربون والجهات التي يتبعونها. وعلى الجانب الآخر فإن هذه

[1] الغافري، المرجع السابق، ص686.

البرامج يمكن أن تفيد متلقي التدريب عن طريق زيادة مهاراته وخبراته ومعلوماته وقدراته على التعامل مع الأجهزة الدولية الأخرى، الأمر الذي ينعكس على الجهة التي ينتمي إليها بالفائدة.

تعد الولايات المتحدة الأمريكية من الدول المتقدمة تكنولوجيا والمتطورة تقنيا في مجال مكافحة الجرائم المعلوماتية وجرائم الشبكات، وعلى الرغم من ذلك فهي تعي وتعلم أنه ما من دولة وإن كانت متقدمة يمكنها التصدي لأخطار هذه الأنماط المستحدثة من الجرائم.

من هذا المنطلق تحرص على الو م أ على توفير المساعدة التقنية والتدريب لرفع قدرات العدالة الجزائية لدى الحكومات الأخرى، ومساعدة ما لديها من أجهزة شرطة، ومسؤولي الادعاء العام، والقضاة ليصبحوا أكثر فعالية في مكافحة الجريمة. فمثل هذه المساعدة لا تؤدي إلى تيسير بناء إطار للتعاون الدولي في مجال تطبيق القانون وحسب، ولكنها تعزز أيضاً قدرة الحكومات الأجنبية المعنية على ضبط مشاكل الجريمة المعلوماتية لديها قبل أن يمتد ليتجاوز حدود بلدانها، فمكتب المساعدة والتدريب على تطوير أجهزة الادعاء العام في الخارج، التابع لوزارة العدل الأميركية، مكلّف تحديداً بتوفير المساعدة اللازمة لتعزيز مؤسسات العدالة الجزائية في دول أخرى، وتعزيز إدارة القضاء في الخارج، كما أن البرنامج الدولي للمساعدة والتدريب على التحقيق الجزائي(ICITAP) الذي كثيراً ما يعمل بالترادف مع وحدته الشقيقة- مكتب المساعدة والتدريب على تطوير أجهزة الادعاء العام في الخارج، العامل داخل وزارة العدل نفسها- على توفير مساعدات لأجهزة الشرطة في البلدان المسماة النامية في مختلف أنحاء العالم، وتهدف المساعدة التي يقدمها هذا البرنامج الأخير إلى تعزيز القدرات التحقيقية لدى أجهزة الشرطة في البلدان الناشئة؛ وفي الوقت الحاضر، تقدّم وزارة العدل الأميركية مساعدات لتطوير القطاع القضائي في عدد من البلدان في أفريقيا، وآسيا، وأوروبا الشرقية والوسطى وأميركا اللاتينية ومنطقة حوض الكاريبي، والدول المستقلة حديثاً، بما ذلك روسيا والشرق الأوسط. مستعينة في ذلك بخبرة الوحدات المتخصصة التابعة لها، هذا من جهة ومن جهة أخرى نجد أن أجهزة تطبيق القانون الأمريكية توفر أيضا تدريبا لنظيراتها من الأجهزة في البلدان الأخرى داخل الولايات المتحدة الأمريكية أو خارجها عن طريق إنشاء معاهد خاصة بتدريب العاملين في أجهزة تطبيق القانون كما هو الحال في كل من المجر، وبوتسوانا، وكوستاريكا، وتايلاند، وفي هذه المعاهد، يقوم خبراء أميركيون في عمل أجهزة تطبيق القانون بإطلاع المتدربين على أساليب وسبل مبتكرة

للتحقيق، ويشجعون على تبادل الآراء مع نظرائهم في مختلف أنحاء العالم[1].

المبحث الثاني: صعوبات التعاون الدولي وسبل التغلب عليها.

يعالج المبحث من خلال التطرق إلى الصعوبات التي تعتري التعاون الدولي في مجال مكافحة الجرائم الواقعة على التجارة الإلكترونية (المطلب الأول)، والجهود المبذولة للتغلب عليها (المطلب الثاني).

المطلب الأول: صعوبات التعاون الدولي في مجال مكافحة الجرائم الواقعة على التجارة الإلكترونية.

يجمع العالم على خطورة الجرائم الواقعة على التجارة الإلكترونية، لما لها من أضرار على الأشخاص والدول، كما يجمع على ضرورة التعاون الدولي للقضاء على هذه الجرائم أو تحجيمها على الأقل إلى أقصى مدى ممكن، بيد أن هناك عقبات تؤثر في فاعلية هذا التعاون، فاختلاف الأنظمة القانونية للدول قد يكون حجر عثرة في مجال مكافحة هذا النوع من الجرائم، لما يترتب عن ذلك من مشكلات تطبيق القانون، وما يثيره من مشكلات ميدانية، كما أن بعض النظم التشريعية لم تواكب بعد التطورات الحاصلة على الصعيد العالمي، فتشريعاتها لم تتطرق بشكل جاد إلى الجرائم الإلكترونية، ولم تعرف هذه الجرائم أو تضع لها نظاما قانونيا خاصا، كما أن مشكلة الإرادة السياسية في مجابهة هذا النوع من الجرائم من الأمور التي ينبغي أخذها في الحسبان.

بناء على ما سبق، يعالج هذا المطلب من خلال التطرق إلى تنازع الاختصاص القضائي (الفرع الأول)، ازدواجية التجريم (الفرع الثاني)، القصور التشريعي لدى بعض الدول والتعارض بين مصالحها (الفرع الثالث)، والاعتبارات السياسية والفنية التي تعيق التعاون الدولي (الفرع الرابع).

[1] الغافري، المرجع السابق، ص ص687-689.

الفرع الأول: تنازع الاختصاص القضائي.

يعني تنازع الاختصاص القضائي، أن الدعوى العمومية قد تقدم عن الجريمة ذاتها أو عدة جرائم مرتبطة ،إلى أكثر من جهة من جهة من جهات التحقيق أو الحكم، فتتمسك كل جهة بالقضية، باعتبار أنها هي المختصة بالنظر فيها، أو ترفض كل واحدة من هذه الجهات النظر على أساس عدم الاختصاص؛ وتسمى الحالة الأولى بتنازع الاختصاص الإيجابي، أما الحالة الثانية فهي تنازع الاختصاص السلبي.

الجرائم الواقعة على التجارة الإلكترونية بصفة خاصة، والجرائم الإلكترونية عامة، من أكبر الجرائم التي تثير مسألة الاختصاص على المستوى الدولي، ولا توجد أي مشكلة بالنسبة للاختصاص على المستوى الوطني أو المحلي حيث يتم الرجوع إلى المعايير المحددة قانونا لذلك.

إن الطبيعة الخاصة لهذه الجرائم كونها عالمية وعابرة للحدود، تثير مشكلة تنازع الاختصاص على المستوى العالمي، بسبب التداخل والترابط بين شبكات المعلومات، فقد تقع الجريمة الإلكترونية في مكان معين، وتنتج آثارها في مكان آخر، سواء داخل الدولة أو خارجها، مما يتسبب في مشكلة البحث عن الأدلة الجنائية على شبكة الانترنت؛ ويشهد الواقع أن مواقع عديدة في دول مختلفة كالصين والكويت وجورجيا وفيتنام قد اخترقت، بل تجرأ البعض وهاجم وكالة الفضاء الأمريكية "ناسا"، خارج دائرة الاختصاص التي قدم فيها البلاغ، أو تم تحريك الدعوى العمومية فيها؛ وكذلك تظهر مشكلات تتعلق بفحص البيانات في مراكز معلومات دول أخرى، وهو ما يتطلب خضوع إجراءات التحقيق للقوانين الجنائية السارية في تلك الدولة.[1]

على المستوى المحلي، تحل مشكل الاختصاص على أساس ما وضعه المشرع وهو مكان القبض على المتهم، أو محل إقامة المتهم، أو مكان وقوع الجريمة، فأي مكان من الأماكن المذكورة ينعقد به الاختصاص القضائي لسلطات التحقيق والمحاكمة.

لكن إذا تعلق الأمر بالاختصاص الدولي فالمسألة تصبح دقيقة، بل معقدة أحيانا، فقد يحدث أن ترتكب الجريمة في إقليم دولة معينة من قبل أجنبي، فهنا تكون الجريمة خاضعة للاختصاص

[1] بيومي حجازي، الجوانب الإجرائية لأعمال التحقيق...المرجع السابق، ص107.

الجنائي للدولة الأولى استنادا إلى مبدأ الإقليمية، وتخضع كذلك لاختصاص الدولة الثانية على أساس مبدأ الاختصاص الشخصي في جانبيه، وقد تكون هذه الجريمة من الجرائم التي تهدد أمن وسلامة دولة أخرى فتدخل عندئذ في اختصاصها استنادا إلى مبدأ العينية، كما تثار فكرة تنازع الاختصاص القضائي في حالة تأسيس الاختصاص على مبدأ الإقليمية، كما لو قام الجاني ببث الصور الخليعة ذات الطابع الإباحي من إقليم دولة معينة وتم الإطلاع عليها في دولة أخرى، ففي هذه الحالة يثبت الاختصاص وفقا لمبدأ الإقليمية لكل دولة من الدول التي مستها الجريمة.[1]

يرى البعض أن حل هذا المشكل المتعلق بتنازع الاختصاص القضائي الدولي، يكون من خلال اعتبار جميع الجرائم الإلكترونية التي تقع في أكثر من دولة، من الجرائم العالمية، تدخل في نطاق الاختصاص القضائي العالمي، أو ما يعرف بالولاية القضائية الكونية، بمعنى أن يعطى الحق للدول بملاحقة ومحاكمة مرتكبي الجرائم العالمية دون أي اعتبار لجنسية مرتكبيها، أو المكان الذي ارتكبت فيه الجريمة، بما مفاده أن ينعقد الاختصاص القضائي الجنائي العالمي لأية دولة ترغب في ملاحقة مرتكبي الجرائم العالمية، ومن أخطرها الجرائم الواقعة على التجارة الإلكترونية؛ ولقد تضمنت العديد من الاتفاقيات الدولية أحكاما تعترف بمبدأ الاختصاص القضائي العالمي، إلا أن جميعها لم تحدد عقوبات معينة لمرتكبي الجرائم العالمية التي تحظرها، ولم تعين جهة قضائية بعينها لمحاكمة المتهمين، ولكنها أكدت فقط على ضرورة سن قوانين لمعاقبة مرتكبي تلك الجرائم، وألزمت الدول بملاحقة الأشخاص المتهمين بارتكاب هذه الجرائم وإحالتهم إلى محاكمها الخاصة، أو تسليمهم لدول أخرى لمحاكمتهم أمام قضائها.[2]

ويرى البعض الآخر من الفقه أن حل مشكلة الاختصاص لا يكون إلا عن طريق الاتفاقيات الدولية، سواء أكانت ثنائية أم جماعية، وتعد اتفاقية بودبست لسنة 2001 مثالا يحتذى به، وقد نصت على الاختصاص القضائي في م22 منها، ونصت في م5/22 على حالة التنازع الإيجابي في الاختصاص القضائي: "في حالة مطالبة أكثر من طرف من الأطراف بالاختصاص القضائي بشأن جريمة ما تقرها هذه الاتفاقية، يقوم الأطراف المعنيون، متى كان ذلك ملائما، بالتشاور بغرض تحديد الاختصاص القضائي الأكثر ملاءمة للمحاكمة".

---

[1] الغافري، المرجع السابق، ص693.

[2] سامح أحمد، المرجع السابق، ص539.

أما الاتفاقية العربية لمكافحة جرائم تقنية المعلومات سالفة الذكر فقد نصت في م3/30 على حالة التنازع الإيجابي للاختصاص القضائي: "إذا ادعت أكثر من دولة طرف بالاختصاص القضائي لجريمة منصوص عليها في هذه الاتفاقية، فيقدم طلب الدولة التي أخلت الجريمة بأمنها أو بمصالحها، ثم الدولة التي وقعت الجريمة بإقليمها، ثم الدولة التي يكون الشخص المطلوب من رعاياها، وإذا اتحدت الظروف، فتقدم الدولة الأسبق في طلب التسليم".

الملاحظ أن التشريعات الجنائية المطبقة حاليا في معظم دول العالم ترتكز على الصفة الإقليمية، فيما يتعلق بتطبيق قواعد الإجراءات الجزائية عن طريق السلطات غير الوطنية، فهي لا تتقدم بالسرعة ذاتها التي تتقدم وتنمو بها حركة الاتصالات والمعلوماتية التي عمت العالم كله، فلا مناص من الاتفاقيات الثنائية أو الجماعية بين الدول لتسهيل إجراءات التحقيق والتقاضي في الجرائم الإلكترونية؛ ورغم إبرام بعض هذه الاتفاقيات فإن ذلك لم يف بالمطلوب لحل مشكلات الاختصاص وتبادل الأدلة وتسليم المجرمين، لذلك بات من الضروري بل من الواجب سن تشريعات جزائية أكثر مرونة لمواكبة سرعة تقدم الحاسب الآلي والانترنت، وإيجاد آليات أكثر ملاءمة للتصدي لهذه الجرائم.[1]

الفرع الثاني: ازدواجية التجريم.

مهما كانت الطريقة المتبعة لتحديد الجرائم التي يجوز بشأنها التسليم، سواء كانت قائمة على نهج الاستبعاد أو على نهج ذكر الجرائم حصريا، فإن كل القوانين والاتفاقيات التي تعرضت لتسليم المجرمين تضمنت شرط التجريم المزدوج للاستجابة لطلبات التسليم؛ ذلك أن التسليم إجراء خطير يمس بالحقوق الشخصية للأفراد المطالب تسليمهم، خاصة إذا تعلق الأمر بقضاء أجنبي، كما أن الشخص وحسب القواعد العامة لا يجوز محاكمته على فعل غير مجرم أو لم يكن مجرما من قبل، وإقدام شخص ما على ارتكاب فعل ما غير مجرم في الدولة التي ارتكب فيها الفعل يعطيه ضمانة قانونية بألا تسلمه هذه الدولة إلى دولة أخرى وإن كان الفعل مجرما عند هذه الأخيرة، حتى لا تصطدم مشاعر أفراد الدولة بالقبض على شخص أو اعتقاله، فقط لأنه ارتكب فعلا تعتبره تلك الدولة مباحا ومشروعا.

[1] بيومي حجازي، المرجع السابق، ص108.

وبالرغم من أهمية شرط التجريم المزدوج، باعتباره ضمانة لحقوق الأفراد، يرى البعض أنه عقبة أمام التعاون الدولي في مجال تسليم المجرمين بالنسبة للجرائم المعلوماتية، سيما وأن كثيرا من الدول لا تجرم هذه الجرائم، بالإضافة إلى أنه من الصعوبة تحديد فيما إذا كانت النصوص التقليدية لدى الدولة المطلوب منها التسليم يمكن أن تنطبق على الجرائم المتعلقة بالتجارة الإلكترونية أم لا، الأمر الذي يعوق تطبيق الاتفاقيات الدولية في مجال تسليم المجرمين، ويحول بالتالي دون جمع الأدلة ومحاكمة مرتكبي الجرائم الإلكترونية عامة.[1]

نصت م2/43 من اتفاقية الأمم المتحدة لمكافحة الفساد على أنه: "في مسائل التعاون الدولي، كلما اشترط توافر ازدواجية التجريم وجب اعتبار ذلك الشرط مستوفيا، بصرف النظر عما إذا كانت قوانين الدولة الطرف متلقية الطلب تدرج الجرم المعني ضمن نفس فئة الجرائم التي تدرجه فيها الدولة الطرف الطالبة، أو تستخدم في تسميته نفس المصطلح الذي تستخدمه الدولة الطرف الطالبة، إذا كان السلوك الذي يقوم عليه الجرم الذي تلتمس بشأنه المساعدة يعتبر فعلا إجراميا في قوانين كلا الطرفين".

هذه المادة وسعت بينت مفهوم ازدواجية التسليم، وأن المراد منه أن يكون الفعل المجرم في كلا الدولتين: طالبة التسليم والمطلوب منها، بغض النظر عن التكييف القانوني في كلا الدولتين للجريمة المرتكبة، أو عن تسميتها.

أما بعض الاتفاقيات الأخرى كاتفاقية جامعة الدول العربية، فقد ذهبت أكثر من هذا، إذ أجازت التخلي عن شرط ازدواجية التجريم، في حالة ما إذا كان الشخص المطلوب من رعايا الدولة طالبة التسليم، أو كان من رعايا دولة أخرى تقرر العقوبة ذاتها.

الفرع الثالث: قصور بعض التشريعات الوطنية.

رغم الجهود الدولية الحثيثة لمجابهة ومكافحة الجرائم الإلكترونية بصفة عامة، وجرائم التجارة الإلكترونية بصفة خاصة، إلا أنها تبقى غير كافية، وتحتاج إلى جهد أكبر، خاصة وأن العديد من الدول لم تستكمل أنظمتها القانونية المتعلقة بالجرائم الإلكترونية، فهناك قصور تشريعي واضح

[1] الغافري، المرجع السابق، ص694.

لدى بعض الدول، التي لم تستطع مسايرة سرعة التقدم المعلوماتي، ومن ثمة الجرائم الإلكترونية، ولا يزال الخلاف الفقهي قائما لدى بعض الدول العربية مثلا بخصوص هذه القوانين، وهل من الأجدى تعديل التشريعات الجزائية القائمة كي تستوعب الجرائم الإلكترونية؟ أم تعدل قوانين حماية الملكية الفكرية كي تستوعب هذه السلوكيات وتجرمها بوصفها أقرب ما تكون إلى حق المؤلف، أم يكون من الملائم إصدار تشريعات جديدة خاصة بالجرائم الإلكترونية؟ وفي بعض الجرائم الإلكترونية، لا يقف الصراع عند هذا الحد، فما يراه البعض جائزا، يراه البعض الآخر غير ذلك، ومرد ذلك إلى طبيعة النظام القانوني السائد في كل بلد من البلدان، رغم المجهودات المبذولة لتوحيد الرؤى وتضافر الجهود بشأن هذه الجرائم، إلا أن الكثير من التشريعات لا زالت في مهدها، ولا يمكن اعتبارها جامعة مانعة، بدليل أن الشركات التجارية لديها مطالب في كل عام بإضافة نماذج من السلوك الإجرامي المعلوماتي لم تكن متضمنة ذي قبل. ولعل عدم الاتفاق بين الأنظمة القانونية المختلفة بالشكل الكافي على صورة موحدة للجرائم الإلكترونية، يغري قراصنة المعلوماتية على تنظيم أنفسهم وزيادة الجرأة لديهم على ارتكاب المزيد من الجرائم دون اعتبار للحدود الجغرافية.[1]

الفرع الرابع: الاعتبارات السياسية والفنية.

إن تغليب الدول لمصالحها السياسية الضيقة على حساب العدالة الجنائية يحول في الكثير من الأحيان دون متابعة مجرمي المعلوماتية؛ فقد تتعارض مصالح بعض الدول مع بعضها البعض، أو تنشأ خلافات سياسية بين بعض الدول – خاصة دول العالم الثالث – مما يجعل هذه الدول لا تتعاون بالشكل المطلوب في مسائل العدالة الجنائية والمساعدة القضائية وتسليم المجرمين، وتزيد هوة فشل التعاون الدولي، عند اختلاف الإيديولوجيات أو نظم القيم، أو في مستويات حقوق الإنسان وحرياته، أو في مستويات العمل الديمقراطي الداخلي، وهذا كله ينعكس سلبا على إجراءات التعاون الدولي.[2]

إن الرغبة في السيادة الإقليمية والوطنية مطلب كل الدول، غير أن مصلحة المجتمع الدولي قد تضطر الدول إلى نظرة أخرى أكثر مرونة بشأن السيادة، من خلال الاتفاقيات التي تحاول أن تراعي جانبين مهمين: سيادة الدول وملاحقة المجرمين، غير أن التوفيق بين هذين الجانبين ليس دائما

[1] بيومي حجازي، المرجع السابق، ص 104.

[2] سامح أحمد، المرجع السابق، ص541.

بالأمر اليسير، وقد أقرت الأمم المتحدة مبدأ التعاون في إطار احترام السيادة والحرمة الإقليمية للدول، وعدم التدخل في شؤونها الداخلية.[1]

ترتبط المصلحة الوطنية بمفاهيم خاصة، قد تكون معوقا من معوقات التعاون الدولي، كما أن تفسير المصلحة الوطنية قد يخضع للسرية من قبل كل دولة، ناهيك عن أن مصطلح المصلحة الوطنية عام وفضفاض وغير مضبوط بدقة ويحتمل تأويلات كثيرة؛ إلا أنه في الدول الديمقراطية فإن المصلحة الوطنية عادة ما تعكس ولاء الحاكم لشعبه، وقد تتعدد تسمياتها من المصلحة الوطنية، إلى المصلحة العامة، إلى المصلحة القومية، إلى المصلحة الشرعية... وتقسم إلى مصلحة وطنية لحماية الأمن القومي، ومصلحة وطنية لحماية المجتمع من التهديدات الخارجية، لذا فإن كل دولة تحرص من حيث الوسائل أو الإجراءات القانونية على ضمان هذه المصالح، مما يعرقل بشكل أو بآخر عملية التعاون الدولي.[2]

كذلك نجد أن الكثير من الدول تفسر بعض الشروط بتوسع، وتعتبر التسليم في العديد من الجرائم الإلكترونية يمس بمصالحها الأساسية أو سيادتها القومية، ولذلك تمتنع عن تسليم المجرم للدولة الطالبة لهذه الأسباب.[3]

وهنالك صعوبات أخرى تقف حجر عثرة أمام التعاون الدولي منها أن أهم الأهداف المرجوة من التعاون الدولي في مجال الجريمة والمجرمين، هو الحصول على المعلومات والبيانات المتعلقة بهم، ولتحقيق هذا الهدف كان لزاما أن يكون هناك نظام اتصال يسمح للجهات القائمة على التحقيق بالاتصال بجهات أجنبية لجمع أدلة معينة أو معلومات مهمة، فعدم وجود مثل هذا النظام يعني عدم القدرة على جمع الأدلة والمعلومات العملية التي غالبا ما تكون مفيدة في التصدي لجرائم معينة ولمجرمين معينين، وبالتالي تقل الفائدة من هذا التعاون.[4]

كما أن الأصل بالنسبة لطلبات الإنابة القضائية الدولية والتي تعد من أهم صور المساعدات القضائية الدولية في المجال الجنائي أن تسلم بالطرق الدبلوماسية، وهذا بالطبع يجعلها

[1] السقا، المرجع السابق، ص523.

[2] المرجع نفسه، ص524.

[3] فريد منعم، المرجع السابق، ص221.

[4] الغافري، المرجع السابق، ص 692.

تتسم بالبطء والتعقيد، والذي يتعارض مع طبيعة الجرائم الإلكترونية وما تتميز به من سرعة، وهو الأمر الذي انعكس على الجرائم المتعلقة بالتجارة الإلكترونية.

كذلك من الصعوبات الكبيرة في مجال المساعدات القضائية الدولية المتبادلة التباطؤ في الرد، حيث أن الدولة متلقية الطلب غالبا ما تكون متباطئة في الرد على الطلب سواء بسب نقص الموظفين المدربين أو نتيجة الصعوبات اللغوية أو الفوارق في الإجراءات التي تعقد الاستجابة وغيرها من الأسباب. ولقد تم شطب الكثير من القضايا لعدم تلبية طلب بسيط في الوقت المناسب[1].

كما أن هنالك صعوبات تتمثل في عدم رغبة بعض القيادات الإدارية في بعض الدول في التدريب، لاعتقادهم بدوره السلبي في تطوير العمل من خلال تطبيق ما تعلمه المتدربون في الدورات التدريبية وما اكتسبوه من خبرات، ومن الصعوبات أيضا والتي قد تهدد التعاون في مجال التدريب ما يتعلق بالفوارق الفردية بين المتدربين وتأثيرها على عملية الاكتساب للمهارات المستهدفة بقوة تامة ومتكافئة لدي مختلف الأفراد المتدربين، سيما في مجال تكنولوجيا المعلومات وشبكات الاتصال حيث أنه يوجد بعض الأشخاص لا كفاءة لهم على الإطلاق في هذا الميدان، وعلى النظير يوجد أناس على درجة كبيرة من المعرفة والثقافة في هذا المجال، بالإضافة إلى أن نظرة المتدرب إلى الدورة التدريبية على أنها مرحلة تدريبية أو عبء لا طائل منه تهدد العملية التدريبية برمتها وبالطبع نسف التعاون الدولي في هذا المجال، أيضا من الصعوبات التي قد تؤثر على العملية التدريبية وعلى التعاون الدولي فيها ما يتعلق بالملامح العامة المميزة للبيئة التدريبية وعدم قدرتها على تمثيل الواقع العملي لبيئة العمل الطبيعية تمثيلا تاما ومتقنا، من حيث ما يدور بها من وقائع وملابسات وإجراءات، وما يتم فيها من نشاطات لا تبلغ حد التطابق مع طبيعة المهام التي سيؤديها المتدربون في بيئة العمل الطبيعية[2].

[1] المرجع نفسه، ص694.

[2] الغافري، المرجع السابق، ص695.

المطلب الثاني: الجهود المبذولة للتغلب على معوقات التعاون الدولي.

يتعين على كل دولة أن تعمل على تدعيم وتفعيل آليات التعاون مع غيرها من دول العالم، عن طريق تغليب المصلحة العامة المشتركة، على المصالح الضيقة لكل دولة، وبذل المزيد من الجهود، على الصعيدين الوطني والدولي، بهدف القضاء أو الحد من الصعوبات التي تعترض التعاون الدولي؛ وعليه يتم دراسة هذا المبحث من خلال التطرق إلى جهود التغلب على صعوبات التعاون الدولي في مكافحة الجرائم الإلكترونية على المستوى الداخلي (الفرع الأول)، ثم الجهود المبذولة على الصعيد الخارجي (الفرع الثاني).

الفرع الأول: الجهود الوطنية للتغلب على معوقات التعاون الدولي.

تتخذ الجهود التي تبذلها كل دولة من الدول للحد من المعوقات التي تعترض سبيل تعاون دولي فعال في مكافحة الجرائم الإلكترونية عامة، والجرائم الواقعة على التجارة الإلكترونية بصفة خاصة، منحيين، المنحى الأول يتعلق بالتدابير الموضوعية، أما المنحى الثاني فيتعلق بالتدابير الإجرائية.[1]

فيما يخص التدابير الموضوعية، يجب على كل دولة اتباع سياسة جنائية تهدف إلى التعاون مع باقي الدول، من خلال تبني تدابير وتشريعات تتلاءم والطبيعة الخاصة للجرائم الإلكترونية، بغية مواجهة مخاطر استخدام تقنيات المعلومات الحديثة في ارتكاب الأفعال الإجرامية، وإمكانية نقل وتخزين الأدلة المتعلقة بالنشاطات الإجرامية، وفقا لما تقضي به أحكام القوانين الداخلية، هذه الأخيرة ينبغي أن تجرم كل الأفعال التي تعتبر اعتداء على التجارة الإلكترونية، وتعاقب عليها عقوبات رادعة، بما يسمح بتوفير حماية جنائية فعالة للتجارة الإلكترونية، ولهذا يتوجب أيضا على الدول أن تجيز في تشريعاتها مساءلة الشخص المعنوي جنائيا عن الجرائم المرتكبة من قبله أو لصالحه بما يتلاءم وطبيعة الشخص المعنوي وكذا الجريمة المرتكبة، وهذا ما دعت إليه م20 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، والتي دعت أيضا في م21 إلى تشديد العقوبات على الجرائم التقليدية في حال ارتكابها بواسطة تقنية المعلومات.

[1] سامح أحمد، المرجع السابق، ص542-543.

أما فيما يخص التدابير الإجرائية، فينبغي على كل دولة أن تتبنى التدابير التشريعية الإجرائية التي تمكنها من تفتيش نظم وشبكات الحاسب الآلي أو أجزائها وفحص البيانات المخزنة بها، أو على الوسائط الملحقة بها، سواء كان محل التفتيش داخل الدولة أم خارجها، بشرط أن يفيد عملية التحقيق في الجريمة ويحترم الضمانات القانونية لمن تم التفتيش قبله، وهذا ما دعت إليه م26 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات،كما يلزم لكل دولة أن تتخذ التدابير التشريعية الإجرائية التي تخول لسلطاتها المعنية صلاحيات ضبط وإحضار المتورطين في الجريمة، سواء تواجدوا في إقليمها أم لا، وتتعاون الدول بينها لتسهيل ذلك، كما يجب على كل دولة أن تتخذ تدابير تشريعية ترمي إلى تمكين سلطاتها المعنية من الحصول على نسخة حفظ سريعة للبيانات المخزنة في أحد أنظمة الحاسب الآلي، بما يحقق مصلحة التحقيقات، وخاصة إذا ما تبين أن تلك البيانات معرضة للفقد أو المحو أو التعديل أو التلف، وهذا ما نصت عليه م37 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، كما تلتزم كل دولة بتبني الإجراءات الضرورية لإلزام شخص بحفظ المعلومات المخزنة والموجودة بحيازته، والعمل على سلامتها لمدة معينة (90 يوما)، وكذا إلزام الشخص المسؤول عن حفظ تقنية المعلومات للإبقاء على سرية الإجراءات طوال الفترة القانونية المنصوص عليها قانونا (م23 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات)، كما ينبغي على كل دولة أن تلتزم بتبني الإجراءات الضرورية لتمكين سلطاتها المختصة من ضبط وتأمين المعلومات المخزنة على الحاسب الآلي أو أحد ملحقاته، وعمل نسخة لها والاحتفاظ بها، والحفاظ على سلامتها (م27 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات)، كما يلزم كل دولة أن تقوم بجمع معلومات تتبع المستخدمين بالتعاون مع مزود الخدمة في حدود اختصاصه، مع إلزامه بالسرية التامة (م28 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات)، كما يلزم كل دولة أن تتبنى تشريعات إجرائية لاعتراض معلومات المحتوى (م29 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات)، كما يجب على الدول أن تتخذ كل الإجراءات لمد اختصاصها على الجرائم الإلكترونية إذا ارتكبت كليا أو جزئيا أو تحققت نتيجتها في إقليم الدولة، أو على متن سفينة تحمل علمها، أو على متن طائرة مسجلة تحت قوانينها، أو من قبل أحد مواطنيها بالخارج، أو إذا مست الجرائم أحد مصالحها العليا (م30 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات).

الفرع الثاني: الجهود الدولية للتغلب على معوقات التعاون الدولي.

ينبغي على الدول التفاوض الجاد للوصول إلى معاهدات واتفاقيات دولية أو إقليمية تضع الإطار العام لمكافحة كل أشكال الجرائم المستحدثة، ومن بينها الجرائم الواقعة على التجارة الإلكترونية، تحتذي به الدول في تعديل تشريعاتها أو استحداث تشريعات جديدة، مثلما كان الشأن بالنسبة لقانون الأونسترال النموذجي بشأن التجارة الإلكترونية لسنة 1996، وكذا قانون الأونسترال النموذجي بشأن التوقيع الإلكتروني لسنة 2001.

فيما يتعلق بالعقبة المتمثلة في عدم وجود نموذج موحد للنشاط الإجرامي فإن الأمر يقتضي توحيد هذه النظم القانونية، غير أن هذا الأمر يبدو ضربا من المستحيلات، لذا لا مناص من البحث عن وسيلة أخرى تساعد على إيجاد تعاون دولي يتفق مع طبيعة هذا النوع المستحدث من الجرائم، ويخفف من شدة الفوارق بين الأنظمة العقابية الداخلة، وتتمثل هذه الوسيلة في تحديث التشريعات المحلية المعنية بالجرائم المعلوماتية و إبرام اتفاقيات خاصة يراعي فيها هذا النوع من الجرائم، كحماية البيانات والخصوصية في إطار القانون الجنائي، والتشفير والتوثيقات الرقمية.

وبالنسبة للمعوق الخاص بتنوع واختلاف النظم القانونية الإجرائية، فإن الصكوك الدولية الصادرة عن الأمم المتحدة غالبا ما تشجع الأطراف فيها على السماح باستخدام بعض تقنيات التحقيق الخاصة، الشيء الذي يخفف من شدة اختلاف النظم القانونية والإجرائية، ويفتح المجال أمام تعاون دولي فعّال؛ فمثلا المادة 20 من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية تشير في هذا الصدد إلى التسليم المراقب، والمراقبة الإلكترونية وغيرها من أشكال المراقبة والعمليات المستترة،[1] والتي تعتبر من أهم التقنيات المستخدمة في التصدي للجماعات الإجرامية المنظمة المحنكة، بسبب الأخطار والصعوبات الكامنة وراء محاولة الوصول إلى عملياتها وتجميع المعلومات وأدلة الإثبات لاستخدامها فيما بعد في الملاحقات القضائية المحلية منها أو الدولية في دول أطراف في سياق نظم المساعدة القانونية المتبادلة،[2] وهذا ما أكدت عليه الاتفاقية الأوربية للإجرام المعلوماتي حيث نصت المادة 29 على سرية حفظ البيانات المعلوماتية المخزنة وأجازت لكل طرف أن يطلب من الطرف الآخر الحفظ السريع للمعلومات المخزنة عن طريق إحدى الوسائل الإلكترونية الموجودة داخل النطاق

[1] المادة 11 من اتفاقية 1988 بشأن التسليم المراقب، والمادة 50 من اتفاقية الأمم المتحدة لمكافحة الفساد.

[2] الغافري، المرجع السابق، ص696.

المكاني لذلك الطرف الآخر والتي ينوي الطرف طالب المساعدة أن يقدم طلباً للمساعدة بشأنها بغرض القيام بالتفتيش أو الدخول بأي طريقة مماثلة، وضبط أو الحصول أو الكشف عن البيانات المشار إليها، وهذا ما أكدت عليه أيضا م3/37 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات سالفة الذكر، كما أكدت المادة 30 من الاتفاقية الأوربية على الكشف السريع عن البيانات المحفوظة حيث نصت على: "عند تنفيذ طلب حفظ البيانات المتعلقة بالتجارة غير المشروعة والمتعلقة باتصال خاص تطبيقاً لما هو وارد في المادة 29 فإن الطرف المساند إذا اكتشف وجود مؤدي خدمة في بلد آخر قد شارك في نقل هذا الاتصال فإن عليه أن يكشف على وجه السرعة إلى الطرف طالب المساعدة كمية كافية من البيانات المتعلقة بالتجارة غير المشروعة حتى يمكن تحديد هوية مؤدي الخدمة هذا والطريق الذي تم الاتصال من خلاله."

كما أشارت المادة 31 من هذه الاتفاقية إلى المساعدة المتعلقة بالدخول إلى البيانات المحفوظة، حيث أجازت لأي طرف أن يطلب من أي طرف آخر أن يقوم بالتفتيش أو أن يدخل بأي طريقة مشابهة وأن يضبط أو يحصل بطريقة مماثلة، وأن يكشف عن البيانات المحفوظة بواسطة شبكة المعلومات داخل النطاق المكاني لذلك الطرف والتي يدخل فيها أيضاً البيانات المحفوظة وفقاً للمادة 29، ويجب الاستجابة لمثل هذا الطلب بأسرع ما يمكن في حالات معينة منها: إذا كانت هناك أسباب تدعو للاعتقاد أن البيانات المعنية عرضة على وجه الخصوص لمخاطر الفقد أو التعديل.

في حين تطرقت المادة 32 من الاتفاقية ذاتها سمحت بالدخول للبيانات المخزنة خارج نطاق الحدود بشرط أن يكون ذلك بموجب اتفاق، أو أن تكون هذه البيانات متاحة للجمهور.

أيضا نصت المادة 33 على تعاون الدول الأطراف فيما بينها لجمع البيانات في الوقت الحقيقي عن التجارة غير المشروعة، والمرتبطة باتصالات خاصة على أرضها تتم بواسطة شبكة معلومات، وفي إطار ما هو منصوص عليه في الفقرة الثانية. وينظم هذا التعاون الشروط والإجراءات المنصوص عليها في القانون الداخلي. ويمنح كل طرف تلك المساعدة على الأقل بالنسبة للجرائم التي يكون جمع المعلومات بشأنها في الوقت الحقيقي متوافر في الأمور المشابهة على المستوى المحلي.

وهناك أيضا المادة 34 من ذات الاتفاقية والتي نصت على التعاون في مجال التقاط البيانات المتعلقة بمضمون الاتصالات النوعية التي تتم عن طريق إحدى شبكات المعلومات.

ونلاحظ مما سبق أن الاتفاقية الأوربية للإجرام المعلوماتي أوجدت بعض الحلول التي من شأنها التغلب على مشكلة اختلاف النظم الإجرائية أمام التعاون الدولي لمواجهة الجرائم المتعلقة بالتجارة الإلكترونية[1].

وللحد من ظاهرة عدم وجود قنوات اتصال بين جهات إنفاذ القانون فنلاحظ أنه غالبا ما تشجع المعاهدات والاتفاقيات الدولية الدول على التعاون فيما بينها وتدعوها إلى إنشاء قنوات اتصال بين سلطاتها المختصة ووكالاتها ودوائرها المتخصصة بغية التيسير في الحصول على هذه المعلومات وتبادلها،[2] ومن الأمثلة على هذه المعاهدات الدولية اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية في المادة 27 منها، والمادة 9 من اتفاقية 1988، والمادة 48 من اتفاقية الأمم المتحدة لمكافحة الفساد، والبند الثاني من المادة 27 من الاتفاقية الأوربية بشأن الإجرام المعلوماتى، والمادة 35 من الاتفاقية الأوربية والتي أوجبت على الدول الأطرف فيها ضرورة تحديد نقطة اتصال تعمل لمدة 24 ساعة يومياً طوال أيام الأسبوع لكي تؤمن المساعدة المباشرة للتحقيقات المتعلقة بجرائم البيانات والشبكات، أو استقبال الأدلة ذات الشكل الإلكتروني، وهذه المساعدة تشمل تسهيل أو – إذا سمحت الممارسات والقوانين الداخلية بذلك– إسداء النصيحة الفنية، حفظ البيانات وفقاً للمواد 29، 30، جمع الأدلة وإعطاء المعلومات ذات الطابع القضائي وتحديد أماكن المشتبه فيهم، كما أوجبت ذات المادة على الدول الأطراف ضرورة أن تتمكن نقطة الاتصال من الاتصال السريع بنقطة اتصال الطرف الآخر، وأن يعمل كل طرف على أن يتوافر لديه الأفراد المدربون القادرون على تسهيل عمل الشبكة.

كما أن م43 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات أكدت على ضرورة وجود جهاز متخصص لدى كل دولة، متفرغ على مدار الساعة لضمان توفير المساعدة الفورية لغايات التحقيق أو الإجراءات المتعلقة بجرائم تقنية المعلومات، أو لجمع الأدلة بشكلها الالكتروني في جريمة معينة، وتشمل هذه المساعدة: توفير المشورة الفنية، حفظ المعلومات، جمع الأدلة وإعطاء المعلومات القانونية وتحديد مكان المشبوهين. وأكدت المادة نفسها على ضرورة أن توفر كل دولة

[1] الغافري، المرجع السابق، ص699.

[2] يراجع مثلا ما جاء في توصية المجلس الأوربي رقم 13(R95) الصادرة في 1999/09/11م بشأن مشاكل الإجراءات الجنائية المتعلقة بتكنولوجيا المعلومات.

العنصر البشري الكفء من أجل تسهيل عمل الجهاز المتخصص.

أما بالنسبة لمشكلة الاختصاص في الجرائم الإلكترونية، فثمة حاجة ملحة إلى إبرام اتفاقيات دولية ثنائية كانت أم جماعية يتم فيها توحيد وجهات النظر فيما يتعلق بقواعد الاختصاص القضائي خاصة بالنسبة للجرائم المتعلقة بالإنترنت.

ولأجل القضاء على مشكلة التجريم المزدوج والذي يعد من أهم الشروط الخاصة بنظام تسليم المجرمين، ركزت الاتجاهات والتطورات التشريعية الخاصة بتسليم المجرمين على تخفيف التطبيق الصارم لهذا الشرط، وذلك بإدراج أحكام عامة في المعاهدات والاتفاقيات المعنية بتسليم المجرمين وذلك إما بسرد الأفعال التي تتطلب أن تجرم كجرائم أو أفعال مخلة بمقتضي قوانين الدولتين معا أو بمجرد السماح بالتسليم لأي سلوك يتم تجريمه ويخضع لمستوى معين من العقوبة في كل دولة.[1]

وفيما يتعلق بالصعوبات الخاصة بالمساعدات القضائية الدولية والتباطؤ في الرد، تبدو الحاجة ملحة إلى إيجاد وسيلة أو طريقة تتسم بالسرعة، تسلم من خلالها طلبات الإنابة كتعين سلطة مركزية مثلا أو السماح بالاتصال المباشر بين الجهات المختصة بنظر مثل هذه الطلبات لنقضي على مشكلة البطء والتعقيد في تسليم طلبات الإنابة، وهذا بالفعل ما أوصي به مؤتمر الأمم المتحدة الحادي عشر لمنع الجريمة والعدالة الجنائية والذي انعقد في بانكوك في الفترة من 18-2005/4/25 حيث أكد على ضرورة تعزيز فعالية السلطات المركزية المعنية الضالعة في أعمال المساعدة القانونية المتبادلة وإقامة قنوات مباشرة للاتصال فيما بينها بغية ضمان تنفيذ الطلبات في الوقت المناسب، الشيء نفسه نجده في البند الثاني من المادة 27 من الاتفاقية الأوربية بشأن الإجرام المعلوماتي، وكذا المادة 35 من ذات الاتفاقية الأوربية، والمادة 43 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، وكذا المادة 34 من الاتفاقية ذاتها والتي أكدت بأن السلطات المركزية تتصل ببعضها البعض مباشرة في مجال التعاون والمساعدة المتبادلة.

أما بالنسبة للرد على طلبات التماس المساعدة فإنه من الضروري الاستجابة الفورية والسريعة على هذه الطلبات، لأجل ذلك تنص غالبية المعاهدات والاتفاقيات الخاصة بالمساعدات القضائية المتبادلة على ضرورة الاستجابة الفورية والسريعة على طلبات التماس المساعدة، وهذا ما

[1] الغافري، المرجع السابق، ص700.

أكدت عليه الفقرة الثالثة من المادة 25 من الاتفاقية الأوربية للإجرام المعلوماتي حيث نصت على أنه " يمكن لكل طرف، في الحالات الطارئة أن يوجه طلباً للمعاونة أو للاتصالات المتعلقة بها عن طريق وسائل الاتصال السريعة مثل الفاكس أو البريد الإلكتروني على أن تستوفي هذه الوسائل الشروط الكافية المتعلقة بالأمن وصحتها (ويدخل ضمن ذلك الكتابة السرية إذا لزم الأمر) مع تأكيد رسمي لاحق إذا اقتضت الدولة المطلوب منها المساعدة في ذلك، وتقوم الدولة بالموافقة على هذا الطلب والرد عليه عن طريق إحدى وسائل الاتصال السريعة.

أما فيما يتعلق بالصعوبات التي تواجه التعاون الدولي في مجال التدريب فإنه يمكن التغلب عليها بإجراء المزيد من الحملات التوعوية للتنبيه بمخاطر الجرائم المعلوماتية والأضرار التي تسببها وبأهمية تدريب رجال العدالة الجزائية على مواجهتها، كما أنه وبمزيد من التنسيق بن الأجهزة المعنية بتدريب رجال تنفيذ القانون إيجاد برامج تدريبية مشتركة تناسب جميع الفئات، هذا بالإضافة إلى القيام ببعض العمليات المشتركة والتي من شأنها صقل مهارات القائمين على مكافحة تلك الجرائم وتقريب وجهات النظر بشأنها[1].

[1] الغافري، المرجع السابق، ص702.

خاتمة

لقد أفرزت ثورة المعلومات والاتصالات أنماطا جديدة من التعاملات التجارية، بدأت تكتسي شيئا فشيئا أهمية قصوى في المجال التجاري بشكل خاص والمجال الاقتصادي بشكل عام، وأخذت التجارة الإلكترونية تتبوأ مكانة مرموقة في حياة الناس والدول، لما تتميز به من خصائص السرعة وقلة التكلفة، غير أن التكنولوجيا كما لها محاسن وإيجابيات جمة، لها أيضا بعض السلبيات، ليست مرتبطة بذاتها، وإنما باستعمالها من قبل البعض ممن يسمون بمجرمي المعلوماتية، ومن أخطر هذه السلبيات ارتكاب هؤلاء المجرمين لجرائم معينة تعرف بالجرائم الإلكترونية، تتخذ من الوسائل الإلكترونية المختلفة أداة للاحتيال والسرقة والابتزاز... وليست التجارة الإلكترونية في مأمن من هذه الجرائم، بل هي أكثر استهدافا من قبلها، خاصة إذا تعلق الأمر بالمشاريع الكبرى التي تعتبر بيئة مناسبة لمجرمي المعلوماتية قصد تحقيق أرباح كبيرة بشكل غير مشروع، مستغلين في ذلك تكتم أصحاب هذه المشاريع عما حاق بهم من ضرر خشية على سمعتهم لدى عملائهم.

أمام هذه الحقائق بات من الضروري تدخل المشرع سواء على المستوى الوطني، أو على المستوى الدولي من خلال الاتفاقيات والمعاهدات، لتوفير حماية قانونية كافية وكاملة للتجارة الإلكترونية، ولن تؤتي هذه الحماية القانونية ثمارها المرجوة إلا بإعمال القواعد القانونية الجزائية باعتبارها الأكثر قدرة على تحقيق الردع الخاص والعام معا، كما ينبغي التعاون الجاد بين مختلف الدول لمتابعة مجرمي المعلوماتية، نظرا للطبيعة الخاصة للجرائم الإلكترونية، حتى لا يفلت مجرم من قبضة العدالة، دون أن يتخذ ذلك ذريعة للمساس بحقوق الأفراد وحرياتهم الشخصية التي تحميها الدساتير والقوانين والمواثيق الدولية، أو حجة لانتهاك سيادة بعض الدول.

بناء على ما تقدم جاءت هذه الدراسة تحت عنوان "الحماية الجزائية للتجارة الإلكترونية"، لتبيان مدى فاعلية هذه الحماية الجزائية في تحقيق الثقة في الاقتصاد الإلكتروني أو الرقمي، محاولة أن تضع يدها على مواطن القوة والخلل في بعض التشريعات، خاصة التشريع الجزائري، مسترشدة في ذلك بما جادت به قرائح تشريعات مقارنة، وما اجتهد بشأنه القضاء من خلال بعض الأحكام ذات

الصلة، وما أعطاه الفقه من حلول لبعض المشكلات. وتم عرض الدراسة من خلال فصل تمهيدي وبابين.

تم التطرق في الفصل التمهيدي إلى ماهية التجارة الإلكترونية، وإلى الجرائم الإلكترونية، باعتبار أن هذه الجرائم تعد بمثابة العدو الأول واللدود للتجارة الإلكترونية، بحيث تم تناول مفهوم التجارة الإلكترونية ومميزاتها، وتم عرض جملة من التعريفات بشأن التجارة الإلكترونية المقدمة سواء من قبل المشرع، القضاء أو الفقه، ومنها أن التجارة الإلكترونية ما هي إلا نوع من التجارة تتم بوسائل إلكترونية لا تقتصر فقط على الانترنت، بل تتعداها إلى كل الوسائل الإلكترونية التي يمكن أن تتم بها هذه التجارة، تعطي هذه الوسائل للتجارة الإلكترونية خصائص ومميزات فريدة من نوعها، مما يستوجب تعاملا قانونيا يتلاءم وهذه الخصوصية.

توصل البحث أيضا أن هناك مجموعة من العوائق والتحديات التي تقف حجر عثرة أمام تقدم التجارة الإلكترونية، منها ما هو نفسي وثقافي، ومنها ما هو تقني صرف، ومنها ما هو تجاري، ومنها ما هو تشريعي، وهذا التحدي الأخير هو الذي حاول البحث إجلاء الغموض عنه، خاصة ما تعلق منه بالجانب الجزائي بشقيه الموضوعي والإجرائي.

كما أشار البحث إلى موضوع الفجوة أو الهوة الرقمية بين دول الشمال ودول الجنوب، ومردها بالخصوص إلى التفاوت الكبير في التقدم التكنولوجي من دولة إلى أخرى، كما أن هناك فجوة رقمية داخل البلد الواحد مردها عدم المساواة في الوصول إلى تكنولوجيا المعلومات بسبب اختلالات التنمية بين مناطق هذا البلد.

تطرق البحث أيضا إلى واقع وآفاق التجارة الإلكترونية بالجزائر، والجهود التي تبذلها بلادنا على مختلف الأصعدة لتطوير وتحسين الخدمات الإلكترونية بصفة عامة.

وتناول البحث في فصله التمهيدي أيضا موضوع الجرائم الإلكترونية، التي تهدد المعاملات الإلكترونية عامة والتجارة الإلكترونية بصفة خاصة، نظرا لما تتميز به هذه الجرائم من خصائص أهمها سرعة ارتكاب الجريمة وسرعة إزالة آثارها، ارتكابها بشكل مستتر، عدم تركها لآثار مادية ملموسة، وطابعها العابر للحدود الوطنية، كما تطرق البحث إلى المجرم المعلوماتي وبين أهم صفاته وخصائصه.

الباب الأول من الدراسة تناول موضوع الحماية الجزائية للتجارة الإلكترونية من الناحية الموضوعية من خلال التعرض إلى أهم الجرائم الواقعة على التجارة الإلكترونية وصورها، سواء في النصوص العامة المتعلقة بجرائم الأموال، أو النصوص المتعلقة بالملكية الفكرية، وخاصة القانون 03-05 المتعلق بحقوق المؤلف والحقوق المجاورة، ومن خلال نصوص أخرى ذات صلة منها قانون حماية المستهلك وقمع الغش، وقانون التوقيع الإلكتروني الجديد رقم 15-04، وبعض القوانين المقارنة خاصة الفرنسية والمصرية كقانون الملكية الفكرية الفرنسي وقانون الثقة في الاقتصاد الرقمي الفرنسي لسنة 2004، وقانون التوقيع الإلكتروني المصري رقم 15 لسنة 2004.

قُسم هذا الباب إلى فصلين، تناول الأول موضوع الحماية الجزائية لمواقع التجارة الإلكترونية على شبكة الانترنت ومحتوياتها، أما الفصل الثاني فتصدى لموضوع الحماية الجزائية للمستهلك الإلكتروني.

وأهم النقاط التي أثارها هذا الباب كانت كالآتي:

– حماية مواقع التجارة الإلكترونية على شبكة الانترنت وغيرها عن طريق تجريم الدخول غير المشروع على هذه المواقع، وفي سبيل ذلك قام المشرع الجزائري بإضافة قسم سابع مكرر إلى قانون العقوبات بالقانون رقم 04-15، تحت عنوان "المساس بأنظمة المعالجة الآلية للمعطيات" حمى من خلاله بطريقة غير مباشرة هذه المواقع، وهذا أسوة بالمشرع الفرنسي، وشملت هذه الحماية عدة جوانب من خلال تجريم العديد من أفعال الاعتداء على أنظمة المعالجة الآلية للمعطيات، إلا أن الملاحظ أن العقوبات المنصوص عليها يجوز وصفها بأنها غير كافية وغير قادرة على تحقيق الردع، خاصة ما تعلق منها بالغرامة المالية، التي يجب أن تكون قيمتها أعلى لتتلاءم وطبيعة هذه الجرائم، كما فعل المشرع الفرنسي، من ذلك مثلا أن القيمة القصوى للغرامة بالنسبة لجريمة الدخول أو البقاء غير المشروعين هي مائة ألف دينار، وهي قيمة ضئيلة، إذا ما قورنت بالقيمة الواردة في القانون الفرنسي والبالغة 30.000 يورو.

– حماية مواقع التجارة الإلكترونية ومحتوياتها عن طريق قوانين الملكية الفكرية، وفي سبيل ذلك بذلت مجهودات معتبرة على الصعيد الدولي، وكذا على الصعيد الوطني، منها إصدار الجزائر للأمر 05/03 سنة 2003 المتعلق بحقوق المؤلف والحقوق المجاورة، وإصدار المشرع المصري لقانون حق المؤلف رقم

82 لسنة 2002، ومن أهم أنواع الحماية الجزائية التي أقرها المشرع المقارن في قانون حماية المؤلف، تجريم التقليد، وكذا الجرائم المشابهة له التي نص عليها كل من المشرع الفرنسي والمصري، ومنها جريمة المساس بحماية تدابير تقنية الحماية والمعلومات، وجريمة الإخلال بواجبات ومسؤولية المنخرطين عبر شبكة الانترنت.

– حماية أسماء النطاق باعتبارها موضوعا حديثا نسبيا، ومثيرا للكثير من الجدل، ومهما كون أسماء النطاق عناوين افتراضية تحدد مواقع المشروعات على الانترنت، مما يلزم الدول بحل المشاكل المتعلقة بها خاصة المنازعات بين أسماء النطاق والعلامات التجارية.

أما الفصل الثاني من هذا الباب فتناول موضوع الحماية الجزائية للمستهلك في مجال التجارة الإلكترونية، وعالج العديد من النقاط من أهمها:

– توفير حماية للمستهلك الإلكتروني ضد الجرائم التقليدية المرتكبة بواسطة الحاسب الآلي، والجرائم المستحدثة.

– أهم جرائم الأموال التقليدية هي السرقة، النصب أو الاحتيال المعلوماتي، التزوير، خيانة الأمانة، والإتلاف.

– تمثل الإشكال الرئيس بالنسبة لهذه الجرائم في محلها، وثار التساؤل حول مدى جواز اعتبار المعلومات أو المكونات المنطقية للحاسب الآلي مالا منقولا يجوز حمايته وفقا لنصوص هذه الجرائم، فقد رفض جانب من الفقه إعمال النصوص التقليدية لهذه الجرائم لحماية المعلومات، خاصة وأن المشرع حينما سن هذه النصوص لم يكن في نيته ذلك، إلا أن الراجح هو جواز إعمالها، لا سيما في ظل غياب نصوص خاصة كفيلة بتحقيق حماية فضلى للمعلومات، في انتظار أن يعدل المشرع هذه القوانين لتستوعب الجرائم المستحدثة، كما فعل المشرع الفرنسي بالنسبة لجريمة الاحتيال، أو إصدار قوانين خاصة تطبق على الجرائم الواقعة على التجارة الإلكترونية.

– تناول الفصل الأول أيضا موضوع الحماية الجزائية للمستهلك من الجرائم المستحدثة، فتطرق إلى ثلاث جرائم مهمة متعلقة بالإعلانات الإلكترونية الكاذبة أو الخادعة، بطاقات الائتمان، والتوقيع الإلكتروني، وتوصل البحث إلى أن هناك بعض الإشكاليات التي ينبغي للمشرع التدخل سريعا لحلها، منها إصدار قوانين جديدة لمعالجة ظاهرة الإعلانات المضللة، وإلى أن يتم ذلك، فإنه

بالإمكان الاستعانة ببعض نصوص الجرائم التقليدية للتصدي لهذه الجريمة، من ذلك القواعد المتعلقة بجريمة النصب، وتلك المتعلقة بجريمة الخداع، كما يمكن إعمال نصوص قانون حق المؤلف والحقوق المجاورة في بعض الحالات، أما بخصوص بطاقات الائتمان، فإنها تلعب دورا رئيسا في التجارة الإلكترونية، خاصة كأداة وفاء، والملاحظ أن المشرع الجزائري لم ينظم بعد بطاقات الائتمان الخاصة بالتجارة الالكترونية لعدم انتشارها ببلادنا، وهذه البطاقات رغم أهميتها إلا أنها ليست آمنة دوما، لذلك أحاطتها مجموعة من القوانين المقارنة بعناية فائقة من خلال تجريم مختلف صور الاعتداءات الممكن وقوعها على هذه البطاقات، والمتمثلة عموما في استخدامها غير المشروع من قبل حاملها، أو من قبل الغير، وفي غياب نصوص خاصة، لا مناص من الرجوع إلى القواعد العامة المتعلقة بالسرقة أو النصب أو خيانة الأمانة، حسب كل حالة على حدة، غير أن الاختلافات الفقهية الكثيرة حول تكييف الاستعمال غير المشروع للبطاقة يستوجب تدخلا تشريعيا بنصوص خاصة لإنهاء الخلاف. وبخصوص التوقيع الإلكتروني فإن له أهمية بالغة في إبرام العقد الإلكتروني على محرر إلكتروني، ولذلك وجبت حمايته جزائيا، وقد تدخل المشرع الجزائري بقانون 15-04 الخاص بالتوقيع والتوثيق الإلكترونيين، لتوفير هذه الحماية، غير أنها لم تشمل كافة صوره، كما أنها لم تعاقب على المحاولة، ولم يخص المشرع الفرنسي التوقيع الإلكتروني بحماية جزائية خاصة لإمكانية حمايته في إطار القواعد العامة لقانون العقوبات من خلال جرائم الاعتداء على أنظمة المعالجة الآلية للمعطيات، وجريمة التزوير، على خلاف بعض التشريعات العربية التي خصت التوقيع الالكتروني بحماية جزائية،كالتشريع التونسي الذي جاء بحماية شملت العديد من الجرائم سواء في إطار النصوص العامة أو في النصوص الخاصة، وجاء بعقوبات مناسبة، كما خصه التشريع المصري بحماية جزائية في إطار قانون رقم 15-2004 المتعلق بالتوقيع الالكتروني في المادتين: 21،23 وشملت تلك الحماية العديد من الجرائم.

وفرت بعض التشريعات المقارنة حماية جزائية للبيانات الاسمية، من ذلك المشرع الفرنسي الذي حماها جزائيا وفق نصوص قانون 1978، الذي أدرجت نصوصه خاصة فيما بعد في قانون العقوبات، من خلال تجريم عدة سلوكيات سلبية وايجابية، وقرر لها عقوبات مناسبة ورادعة كانت في أغلبها الحبس إلى خمس سنوات والغرامة 300 ألف يورو، كما عاقب عليها ولو بالإهمال، وكذلك جاء التشريع الجزائري بحماية جزائية خاصة للبيانات الشخصية في إطار قانون العقوبات، لكنها غير كافية، ورغم ذلك عاقب على الشروع وجعل صفح الضحية جائزا أمام المتابعة، وعلى خلاف ذلك

جاء التشريع التونسي بحماية جزائية أفضل كونها واسعة النطاق، وكانت الغرامات ملائمة وصلت إلى 100 ألف دينار في جريمة الإفشاء، وقصر العقاب على مزودي الخدمات أو أحد أعوانهم دون غيرهم.

نظمت بعض التشريعات الأوربية بعض القواعد الخاصة بالمسؤولية الجزائية بوسطاء الانترنت تتمشى مع القواعد العامة كاحترامها لقرينة البراءة من خلال تكليف النيابة العامة بإثبات أدلة الإدانة، واحترام مبدأ شخصية العقوبة، كما تطرق المشرع الجزائري إلى مسؤولية الوسطاء في إطار قانون 09-04، وتطرق أيضا إلى مسؤولية مزودي الخدمات في القانون 15-04 الخاص بالتوقيع والتوثيق الإلكترونيين، والتشريع التونسي في إطار قانون المبادلات والتجارة الالكترونية لسنة 2001، وتعد تلك الجهود خطوة جريئة، لكنها غير كافية، كونها ضيقت من نطاق المسؤولية الجزائية وقصرتها على جرائم قليلة، كما افتقرت إلى عقوبات ملائمة خاصة في جريمة الإفشاء.

أما الباب الثاني من الموضوع فقد خصص للقواعد الإجرائية المتعلقة بالتجارة الإلكترونية، وقسم بدوره إلى فصلين، تناول الأول الحماية الجزائية الإجرائية للتجارة الإلكترونية في التشريعات الوطنية، وتطرق الفصل الثاني إلى التعاون الدولي في مجال مكافحة جرائم التجارة الإلكترونية.

وأهم النقاط التي عالجها هذا الباب كانت كالآتي:

- أهمية ودور الضبط الإداري وخاصة الضبط الاقتصادي في حماية التجارة الإلكترونية.

- الضبط القضائي ودوره في التصدي للجرائم الواقعة على التجارة الإلكترونية، وإعطاء الضبطية القضائية بعض الصلاحيات المميزة تتلاءم وطبيعة الجرائم الإلكترونية، وضرورة تقيد رجال الضبطية القضائية بالإجراءات المشروعة والابتعاد عن كل الإجراءات غير المشروعة، حتى لا تكون معيبة بما يبطلها، وعموما فإن معظم التشريعات المقارنة قد أجازت التحريات التي لا تتعلق بحرمة الحياة الخاصة، وتقدير ذلك مسألة موضوعية متروكة للقضاء. ونظرا لخصوصية الجرائم الإلكترونية فقد أحدثت التشريعات المقارنة آليات كفيلة للتصدي لها من ذلك المكتب المركزي لمكافحة الإجرام المرتبط بتكنولوجيا المعلومات والاتصال بفرنسا، الإدارة العامة للتوثيق والمعلومات بمصر، وأنشأت

الجزائر على مستوى الدرك الوطني مركزا لمكافحة جرائم الانترنت، بالإضافة إلى هيئات أخرى، مثل الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، وسلطات التصديق الإلكتروني.

– التحقيق في الجرائم الواقعة على التجارة الإلكترونية، ويتميز بصعوبة كشف الجرائم الواقعة عليها نظرا لطبيعة الجرائم الإلكترونية، وإحجام المجني عليهم عن الإبلاغ.

– نص المشرع الجزائري صراحة على جواز تفتيش المنظومة المعلوماتية في م05 من القانون 09-04 وقد قطع بذلك الخلاف الفقهي حول جواز تفتيش المكونات المعنوية للحاسب الآلي من عدمه، كما أجاز المشرع الجزائري على غرار بعض التشريعات المقارنة التفتيش ولو عن بعد، كما أجاز لقاضي التحقيق القيام بأية عملية تفتيش أو حجز، ليلا ونهارا إذا تعلق الأمر ببعض الجرائم، ومنها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.

– فرضت طبيعة الجرائم الإلكترونية نفسها على المشرع في القانون المقارن، أن يستحدث إجراءات جديدة للتصدي لهذا النوع من الجرائم، ولقد تطرق المشرع الجزائري في قانون الإجراءات الجزائية والقانون 09-04 إلى بعض هذه الإجراءات، ومنها التسرب، التحفظ العاجل على البيانات المخزنة، حفظ المعطيات المتعلقة بحركة السير، الأمر بتقديم بيانات إلكترونية متعلقة بالمشترك، و مراقبة الاتصالات الإلكترونية.

– تحديد المحكمة المختصة في الجرائم الواقعة على التجارة الإلكترونية، إذ أن هذه الجرائم عابرة للحدود أو عالمية، ولا تخرج المواقف التشريعية للدول عن أربعة مبادئ هي: مبدأ الإقليمية، مبدأ العينية، مبدأ الشخصية، ومبدأ عالمية الاختصاص، بخصوص الجرائم الإلكترونية عامة، والجرائم الواقعة على التجارة الإلكترونية بصفة خاصة فهي جرائم لا تعترف بالحدود الإقليمية، مما يدعو إلى القول بملاءمة مبدأ العالمية لهذا النوع المستحدث من الجرائم. ولم يتبن المشرع الجزائري هذا المبدأ رغم أهميته.

– سلطة القاضي الجزائي في قبول الدليل الإلكتروني وتقديره.

–إن الدليل الإلكتروني دليل علمي يجب لزوم تجاوبه مع الحقيقة كاملة وفقا لقاعدة في القضاء المقارن، هي قاعدة أن القانون مسعاه العدالة، أما العلم فمسعاه الحقيقة، لذلك يجب ألا يتعارض الدليل الإلكتروني مع القاعدة العلمية السليمة.

– التعاون الدولي لمكافحة الجرائم الواقعة على التجارة الإلكترونية.

بناء على ما سبق، يُقترح ما يلي:

– اعتبار المال المعلوماتي المعنوي كالبرامج والمعلومات على قدم المساواة في الحماية الجزائية مع الأموال المنصوص عنها في قوانين العقوبات التقليدية، وضرورة التوسيع في مفهوم المحرر محل جريمة التزوير في التشريع الجزائري كما فعلت بعض التشريعات الأجنبية كالتشريع الفرنسي.

– إعادة النظر في حماية المواقع والحماية الجزائية للبيانات الشخصية في التشريع الجزائري، بتوسيع نطاقها من حيث الجرائم، وتقرير عقوبات مناسبة وأكثر ردعا، وتقرير حماية جزائية خاصة لبطاقات الدفع والسحب في التشريع الجزائري، أو تعديل النصوص القائمة لتشمل جميع صور الاعتداء على هذه البطاقات.

– دعوة المشرع الجزائري إلى ضرورة توفير مزيد من الحماية الجزائية للتجارة الالكترونية من خلال المراجعة المستمرة للتشريعات والأنظمة القانونية القائمة لتواكب التطور المستمر في التكنولوجيا.

– ضرورة سن تشريعات عقابية جديدة أو تعديل بعض النصوص التقليدية لمواجهة الجرائم المعلوماتية، وعلى الأخص الجرائم الماسة بالتجارة الالكترونية مثل جرائم الاعتداء على المواقع الالكترونية ذات النشاط التجاري مع تعديل النصوص الجنائية الإجرائية لتتماشى مع روح تطبيق النصوص العقابية.

– ضرورة الإسراع بإصدار تشريع شامل لتنظيم التجارة الالكترونية حماية للاقتصاد القومي في بلداننا العربية وتدعيما لسرعة الاندماج في الاقتصاد الرقمي، وتطوير القوانين الوطنية العربية لتتماشى مع متطلبات نظام التجارة الالكترونية، والاستفادة من التجارب التشريعية للقوانين المقارنة سواء التي تنتمي للمدرسة الأنجلوسكسونية كالقانون الأمريكي، أو التي تنتمي للمدرسة اللاتينية كالقانون الفرنسي.

– ضرورة سن المشرع العربي في كل دولة عربية لقانون خاص بحماية المستهلك، كما هو الحال في التشريعات المقارنة مثل فرنسا، على أن يتضمن هذا القانون نصوصا تعالج الجوانب القانونية التي تحمي المستهلك عند تعاقده عن بعد، وإضافة بنود جديدة تصب في هذا الإطار، بالنسبة لقوانين

الاستهلاك التي تفتقر لذالك، كما هو الحال بالنسبة للتشريع المصري رقم 67 لسنة 2006 بشأن حماية المستهلك الذي يخلو من نصوص قانونية في هذا الصدد.

– وجوب التطوير المستمر للتشريعات المتعلقة بالملكية الفكرية، حماية للحقوق المتعلقة بها، بما يتلاءم مع البيئة الرقمية التي برزت فيها صور جديدة من صور الملكية الأدبية وكذا الملكية الصناعية، وضرورة سن قوانين عربية لتحديد إجراءات تسجيل أسماء الحقول، وبيان العقوبات الواجبة التطبيق في حالة عدم التقيد بها، وكذا تجريم كل صور الاعتداء على هذه الأسماء.

– إدخال موضوع التجارة الالكترونية وأساليب تنظيمها وحمايتها ضمن المناهج الدراسية لكليات الحقوق في جامعات الدول العربية، وإيجاد وعي عام في الدول العربية بضرورة استغلال الإمكانات الهائلة التي تتيحها التجارة الالكترونية، خصوصا للشركات الصغيرة والمتوسطة، في ظل احتدام المنافسة التجارية الدولية في عصر العولمة، وضرورة إجراء المزيد من الدراسات والأبحاث وعقد الندوات المتعلقة بالتجارة الالكترونية، وكيفية مواجهة الأنشطة الإجرامية المرتبطة بها.

– الدعوة إلى صدور قانون دولي موحد خاص بشبكة الانترنت يعنى بتنظيم الانترنت ومحتوى الخدمات والمعلومات فيها، يكون في إطار منظمة الأمم المتحدة.

– الإسراع بالانضمام إلى الاتفاقيات الدولية الخاصة بمكافحة الجرائم المعلوماتية وخاصة المعاهدة الدولية لمكافحة الجرائم المعلوماتية والانترنت.
– اتخاذ التدابير اللازمة لحل مشكلات الاختصاص القانوني والقضائي التي تثيرها الجرائم المعلوماتية.

– ضرورة تعزيز التعاون والتنسيق الدولي بين الدول مع بعضها بعضا، وبين الدول مع المؤسسات الدولية المعنية بهذه المشكلة وبخاصة الانتربول سواء في مجال المساعدات القضائية المتبادلة أو في مجال تسليم المجرمين أو في مجال التدريب؛ والعمل على دراسة ومتابعة المستجدات في هذا المجال على الساحة العالمية.

– دعوة الدول العربية لبناء أنظمة للإنذار المبكر لمواجهة كل أشكال الجريمة المعلوماتية ذات التأثير على المستوى الوطني.

– دعوة وسائل الإعلام لإبراز الدور الهام لمكافحة الجرائم المتعلقة بالتجارة الإلكترونية، وإبراز دور التشريعات العربية بهذا الشأن.

– إيجاد قضاء متخصص للنظر في الجرائم المعلوماتية ومن بينها الجرائم المتعلقة بالتجارة الإلكترونية، وذالك لصعوبة كشف هذه الجرائم وإثباتها والتحقيق فيها وحاجتها إلى معطيات خاصة قد لا تتوافر في القضاء العادي.

– تعزيز وتنشيط تبادل المعلومات بين الأجهزة المنوط بها تنفيذ القانون وهي الشرطة والادعاء العام والقضاء من جهة، وبين خبراء نظم المعلومات من جهة أخرى، بهدف معرفة أبعاد الجرائم المعلوماتية ومقدار الأضرار الناشئة عنها وسمات مجرميها وأساليب منع ارتكابها وملاحقة مرتكبيها.

– وضع سياسة أمنية محكمة لأجل المحافظة على أمن وسلامة وسرية المعلومات.

– إجراء دراسات علمية نفسية، واجتماعية لمعرفة المزيد عن الدوافع الإجرامية لدى مجرمي المعلوماتية، ومحاولة استقطاب النوابغ منهم للعمل ضد الإجرام، مع المؤسسات الأمنية.

– ضرورة أن يتضمن القانون رقم 15-04 المتعلق بالتوقيع والتصديق الإلكترونيين جميع صور الحماية للتوقيع والتصديق الإلكترونيين.

تم بحمد الله تعالى

سيدي بلعباس في 10 جوان 2015.[1]

[1] نوقشت هذه الأطروحة بتأريخ 2015/12/08 بمكتبة كلية الحقوق والعلوم السياسية، جامعة جيلالي ليابس، سيدي بلعباس.

قائمة المراجع

المراجع باللغة العربية

أولا: الكتب العامة:

1- إبراهيم بلعيات، أركان الجريمة وطرق إثباتها في قانون العقوبات الجزائري، دار الخلدونية، الجزائر 2007.

2- د. إبراهيم الشباصي، الوجيز في شرح قانون العقوبات الجزائري، القسم العام، دار الكتاب اللبناني، بيروت، لبنان (دون ذكر سنة النشر).

د. أحسن بوسقيعة، الوجيز في القانون الجزائي العام، ط4، دار هومة، الجزائر 2006.

3- د. أحسن بوسقيعة، الوجيز في القانون الجزائي الخاص، ج1، ط4، دار هومة، الجزائر 2006.

4- د. أحسن بوسقيعة، الوجيز في القانون الجزائي الخاص، الجزء الثاني. ط3، دار هومة، الجزائر 2006.

5- أحمد أبو الروس. جرائم التزييف والتزوير والرشوة واختلاس المال العام من الوجهة القانونية والفنية. المكتب الجامعي الحديث، الأزاريطة، الإسكندرية (بدون سنة نشر).

6- د. أسامة عبد الله قايد، الوسيط في شرح قانون الإجراءات الجنائية المصري، دار النهضة، القاهرة 2007.

7- أعمر قادري، أطر التحقيق، دار هومة، الجزائر 2013.

8- د. باسم شهاب، مبادئ القسم العام لقانون العقوبات، د م ج، وهران 2007.

9- دردوس مكي، القانون الجنائي الخاص في التشريع الجزائري، الجزء الأول، ديوان المطبوعات الجامعية، الجزائر 2005.

10- د. رمسيس بهنام، قانون العقوبات، جرائم القسم الخاص، منشأة المعارف، الإسكندرية، مصر (دون ذكر سنة النشر).

11- د. رؤوف عبيد، مبادئ الإجراءات الجنائية في القانون المصري، ط17، دار الجيل للطباعة، الفجالة، مصر 1989.

12- د. سليمان عبد المنعم، أصول الإجراءات الجزائية في التشريع والقضاء والفقه، المؤسسة الجامعية للدراسات والنشر والتوزيع، بيوت، لبنان 1997.

13- طاهر جليل الحبوش. جرائم الاحتيال. الأساليب والوقاية والمكافحة. أكاديمية نايف العربية للعلوم الأمنية. الرياض 2001.

14- د. عبد الغني بسيوني عبد الله، النظرية العامة في القانون الإداري، منشأة المعارف بالإسكندرية، مصر 2003.

15- د. عبد الفتاح مراد، موسوعة النيابات والتحقيق الجنائي والفني والتصرف في التحقيق، الجزء الأول (دون ذكر سنة النشر ولا دار النشر).

16- العربي بلحاج، أبحاث ومذكرات في القانون والفقه الإسلامي، ج1، د م ج، بن عكنون، الجزائر .1996

17- د. علي عبد القادر القهوجي، شرح قانون العقوبات، القسم العام، المسؤولية الجنائية والجزاء الجنائي، منشورات الحلبي الحقوقية، بيروت، لبنان (دون ذكر سنة النشر).

18- د. علي عبد القادر القهوجي، شرح قانون العقوبات، القسم العام، النظرية العامة للجريمة، دار الهدى للمطبوعات، الإسكندرية، مصر 2002.

19- د. فوزية عبد الستار، شرح قانون العقوبات، القسم الخاص، دار النهضة العربية، القاهرة، الطبعة الثالثة 1990.

20- محمد حزيط، مذكرات في قانون الإجراءات الجزائية الجزائري، ط3، دار هومة، الجزائر 2008.

21- د. محمد زكي أبو عامر، قانون العقوبات، القسم العام، دار الجامعة الجديدة، الإسكندرية، مصر 2007.
22- د. محمد زكي أبو عامر، الإجراءات الجنائية، دار الجامعة الجديدة للنشر، الإسكندرية، مصر 2008.

ثانيا: الكتب المتخصصة.

1- د. أحمد خليفة الملط، الجرائم المعلوماتية، دراسة مقارنة، الطبعة الثانية، دار الفكر الجامعي، الإسكندرية، مصر 2006.

2- د. أحمد محمود مصطفى، جرائم الحاسبات الآلية في التشريع المصري، دراسة مقارنة، دار النهضة، القاهرة 2010.

3- أحمد محمود موافي، الجرائم الإلكترونية وشبكة الانترنت، الناشرون المتحدون، القاهرة (دون ذكر سنة النشر).

4- إدريس النوازلي، الإثبات الجنائي لجرائم الأعمال بالوسائل الحديثة ج1، المطبعة والوراقة الوطنية مراكش، المملكة المغربية 2014.

5- إدريس النوازلي، الإثبات الجنائي لجرائم الأعمال بالوسائل الحديثة ج2، المطبعة والوراقة الوطنية مراكش، المملكة المغربية 2014.

6- إدريس النوازلي، حماية عقود التجارة الإلكترونية في القانون المغربي، المطبعة والوراقة الوطنية مراكش، المملكة المغربية 2010.

7- أمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، ط2، دار هومة، الجزائر 2007.

8- أمير فرج يوسف، التوقيع الإلكتروني، دار المطبوعات الجامعية، الإسكندرية، مصر 2008.

9- د. أمير فرج يوسف، بطاقات الائتمان والحماية الجنائية لها، دار المطبوعات الجامعية، الإسكندرية، مصر 2008.

10- د. الأنصاري حسن النيداني، القاضي والوسائل الإلكترونية الحديثة، دار الجامعة الجديدة، الإسكندرية، مصر 2009.

11- د. إيمان مأمون، أحمد سليمان، إبرام العقد الإلكتروني وإثباته، دار الجامعة الجديدة، الإسكندرية، مصر 2008.

12- د. أيمن رمضان محمد أحمد، الحماية الجنائية للتوقيع الإلكتروني، دار النهضة العربية، القاهرة 2001.

13- د. إيهاب فوزي السقا، الحماية الجنائية والأمنية لبطاقات الائتمان، دار الجامعة الجديدة، الإسكندرية، مصر 2007.

14- د. إيهاب فوزي السقا، جريمة التزوير في المحررات الإلكترونية، دار الجامعة الجديدة، الإسكندرية، مصر 2008.

15- بن زيطة عبد الهادي، حماية برامج الحاسوب في التشريع الجزائري، دار الخلدونية، الجزائر 2007.

16- د. بولين أنطنيوس أيوب، الحماية القانونية للحياة الشخصية في مجال المعلوماتية، منشورات الحلبي الحقوقية، عمان الأردن (دون ذكر سنة النشر).

17- د. ثروت عبد الحميد، التوقيع الإلكتروني، دار الجامعة الجديدة، الإسكندرية، مصر 2007.

18- جلال محمد الزعبي، أسامة أحمد المناعسة، جرائم تقنية نظم المعلومات الإلكترونية، دراسة مقارنة، دار الثقافة، عمان، الأردن .2010

19- أ. د. جميل عبد الباقي الصغير، الانترنت والقانون الجنائي، دار النهضة العربية، القاهرة، مصر 2012.

20- جهاد رضا الحباشنة، الحماية الجزائية لبطاقات الوفاء، دار الثقافة، عمان، الأردن 2008.

21- د. حسين بن سعيد الغافري، السياسة الجنائية في مواجهة جرائم الانترنت، دراسة مقارنة، دار النهضة العربية، القاهرة 2009.

22- خالد حربي السعدي، جريمة إتلاف برامج ومعلومات الحاسب الآلي، دار النهضة العربية، القاهرة 2012.

23- د. خالد محمد كدفور المهيري، جرائم الكمبيوتر والانترنت والتجارة الالكترونية، ط2، معهد القانون الدولي، دار الغرير، دبي، الإمارات العربية المتحدة (دون ذكر سنة النشر).

24- د. خالد ممدوح إبراهيم، أمن الجريمة الإلكترونية، الدار الجامعية، الإسكندرية، مصر 2008.

25- د.خالد ممدوح إبراهيم، حجية البريد الإلكتروني في الإثبات، دراسة مقارنة، دار الفكر الجامعي، الإسكندرية، مصر2010.

26- د.خالد ممدوح إبراهيم، التقاضي الإلكتروني، دار الفكر الجامعي، الإسكندرية، مصر 2008.

27- د.خالد ممدوح إبراهيم، حماية المستهلك في العقد الإلكتروني، دار الفكر الجامعي، الإسكندرية، مصر 2008.

28- د. خالد ممدوح إبراهيم، الجرائم المعلوماتية، دار الفكر الجامعي، الإسكندرية، مصر 2009.

29- د. خالد ممدوح إبراهيم، حقوق الملكية الفكرية، الدار الجامعية، الإسكندرية، مصر 2011.

30- د. خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، دار الفكر الجامعي، الإسكندرية، مصر 2010.

31- د. سعيد السيد قنديل، التوقيع الإلكتروني، الطبعة الثانية، دار الجامعة الجديدة، الإسكندرية، مصر .2006

32- سليم سعداوي، عقود التجارة الإلكترونية، دراسة مقارنة، دار الخلدونية، القبة، الجزائر، 2008.

33- د. شريف محمد غنام، حماية العلامات التجارية عبر الانترنت في علاقتها بالعنوان الالكتروني، دار الجامعة الجديدة، الإسكندرية، مصر 2007.

34- د. شريف محمد غنام، التنظيم القانوني للإعلانات التجارية عبر شبكة الانترنت، دار الجامعة الجديدة، الإسكندرية، مصر 2011.

35- د. طارق عبد العال حماد، التجارة الإلكترونية، الطبعة الثانية، دار الجامعة الجديدة، الإسكندرية، مصر 2007.

36- عائشة بن قارة، حجية الدليل الإلكتروني في مجال الإثبات الجنائي، دار الجامعة الجديدة، الإسكندرية، مصر 2010.

37- د. عامر محمود الكسواني، التجارة عبر الحاسوب، دار الثقافة، عمان، الأردن 2009.

38- د. عبد الفتاح بيومي حجازي، الإثبات الجنائي في جرائم الكمبيوتر والانترنت، دار الكتب القانونية، المحلة الكبرى، مصر 2007.

39- د. عبد الفتاح بيومي حجازي، التوقيع الإلكتروني في النظم القانونية المقارنة، دار الفكر الجامعي، الإسكندرية، مصر 2005.

40- د. عبد الفتاح بيومي حجازي، الجوانب الإجرائية لأعمال التحقيق الابتدائي في الجرائم المعلوماتية، دار النهضة العربية، القاهرة 2009.

41- د. عبد الفتاح بيومي حجازي، مقدمة في حقوق الملكية الفكرية وحماية المستهلك في عقود التجارة الالكترونية، دار الفكر الجامعي، الإسكندرية، مصر 2005.

42- د. عبد الفتاح بيومي حجازي، الجرائم المستحدثة في الجرائم المستحدثة في نطاق تكنولوجيا الاتصالات الحديثة، دار النهضة العربية، القاهرة 2009.

43- د. عبد الفتاح بيومي حجازي، التجارة الإلكترونية وحمايتها القانونية، الكتاب الأول، نظام التجارة الإلكترونية وحمايتها المدنية، دار الكتب القانونية، المحلة الكبرى، مصر 2007.

44- د. عبد الفتاح بيومي حجازي، التجارة الإلكترونية وحمايتها القانونية، الكتاب الثاني، الحماية الجنائية لنظام التجارة الإلكترونية، دار الكتب القانونية، المحلة الكبرى، مصر 2007.

45- عبد الله أحمد عبد الله غرايبة، حجية التوقيع الإلكتروني في التشريع المعاصر، دار الراية، عمان، الأردن 2008.

46- عبد الله عبد الكريم عبد الله، جرائم المعلوماتية والانترنت، منشورات الحلبي الحقوقية، بيروت، لبنان 2007.

47- د. عبد الله عبد الكريم عبد الله، الحماية القانونية لحقوق الملكية الفكرية على شبكة الانترنت، دار الجامعة الجديدة، الإسكندرية، مصر 2008.

48- د. عصام عبد الفتاح مطر، التجارة الالكترونية في التشريعات العربية والأجنبية، دار الجامعة الجديدة، الإسكندرية، مصر 2009.

49- د. عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية، منشأة المعارف، الإسكندرية، مصر (دون ذكر سنة النشر).

50- د. علاء عبد الباسط خلاف، الحماية الجنائية للحاسب الإلكتروني والانترنت، ط2، معهد الكويت للدراسات القضائية والقانونية، الكويت 2009.

51- د. علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب الآلي، دار الجامعة الجديدة، الإسكندرية، مصر 2010.

52- د. عماد مجدي عبد الملك، جرائم الكمبيوتر والانترنت، دار المطبوعات الجامعية، الإسكندرية، مصر 2011.

53- د. عيسى غسان ربضي، القواعد الخاصة بالتوقيع الإلكتروني، دار الثقافة، عمان، الأردن 2009.

54- د. غسان رباح، الوجيز في قضايا حماية الملكية الفكرية والفنية، دراسة مقارنة مع الجرائم المعلوماتية، منشورات الحلبي الحقوقية، بيروت، لبنان 2008.

55- د. غنام محمد غنام، دور قانون العقوبات في مكافحة جرائم الكمبيوتر والانترنت، دار الفكر والقانون، المنصورة، مصر 2013.

56- د. فاتن حسين حوى، المواقع الإلكترونية وحقوق الملكية الفكرية، دار الثقافة للنشر والتوزيع عمان، الأردن، ط2010.

57- د. فؤاد بن صغير، الإجرام الإلكتروني، مطبعة النجاح الجديدة، الدار البيضاء، المغرب 2011.

58- كميت طالب البغدادي، الاستخدام غير المشروع لبطاقة الائتمان، المسؤولية المدنية والجزائية، دار الثقافة، عمان، الأردن 2008.

59- كوثر مازوني، الشبكة الرقمية وعلاقتها بالملكية الفكرية، دار هومة للطباعة والنشر والتوزيع، الجزائر 2008.

60- محمد إبراهيم أبو الهيجاء، عقود التجارة الالكترونية، دار الثقافة، عمان، الأردن 2005.

61- محمد أمين أحمد الشوابكة، جرائم الحاسوب والانترنت، دار الثقافة للنشر والتوزيع، عمان، الأردن 2004.

62- محمد أمين الرومي، النظام القانوني للتوقيع الإلكتروني، دار الكتب القانونية، المحلة الكبرى، مصر 2008.

63- د. محمد حسام محمود لطفي، حقوق الملكية الفكرية، المفاهيم الأساسية، ط2، (دون ذكر دار النشر)، القاهرة 2012.

64- محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، دار الجامعة الجديدة، الإسكندرية، مصر 2007.

65- د. محمد زكي أبو عامر، الحماية الجنائية للحرية الشخصية، دار الجامعة الجديدة، الإسكندرية، مصر 2011.

66- د. محمد زكي أبو عامر، الإثبات في المواد الجنائية، دار الجامعة الجديدة، الإسكندرية، مصر 2011.

67- د. محمد سعيد أحمد إسماعيل، أساليب الحماية القانونية لمعاملات التجارة الإلكترونية، دراسة مقارنة، منشورات الحلبي الحقوقية، بيروت، لبنان 2009.

68- د. محمد السيد عرفة، تدريب رجال العدالة وأثره في تحقيق العدالة، جامعة نايف العربية للعلوم الأمنية ، الرياض 2005.

69- أ.د. محمد الصيرفي، التجارة الإلكترونية، مؤسسة حورس الدولية للنشر والتوزيع، الإسكندرية، مصر 2005.

70- د. محمد فواز المطالقة، الوجيز في عقود التجارة الإلكترونية، دراسة مقارنة، الطبعة الأولى، الإصدار الثاني، عمان، الأردن 2008.

71- د. محمد نور الدين سيد عبد المجيد، المسؤولية الجنائية عن الاستعمال غير المشروع لبطاقات الوفاء والائتمان، دراسة مقارنة، دار النهضة العربية، القاهرة 2008.

72- د. محمد نور الدين سيد عبد المجيد، المسؤولية الجنائية عن تزوير بطاقات الائتمان، دار النهضة العربية، القاهرة 2012.

73- د. محمد نور برهان، د. عز الدين خطاب، التجارة الإلكترونية، الشركة العربية المتحدة للتسويق والتوريدات، مصر الجديدة، القاهرة 2008.

74- د. محمود أحمد طه، المواجهة التشريعية لجرائم الكمبيوتر والانترنت، دار الفكر والقانون، المنصورة، مصر 2013.

75- د. محمود عبد الرحيم الديب، الحماية القانونية للملكية الفكرية في مجال الحاسب الآلي والانترنت، دار الجامعة الجديدة، الإسكندرية، مصر 2005.

76- مختار شبيلي، الإجرام الاقتصادي والمالي الدولي وسبل مكافحته، ط2، دار هومة، الجزائر 2012.

77- د. مدحت عبد الحليم رمضان، الحماية الجنائية للتجارة الإلكترونية، دراسة مقارنة، دار النهضة، القاهرة 2012.

78- أ. د. مصطفى كمال طه، وائل أنور بندق، الأوراق التجارية ووسائل الدفع الإلكترونية الحديثة، دار الفكر الجامعي، الإسكندرية، مصر 2006.

79- د. مصطفى معوان، التجارة الإلكترونية ومكافحة الجريمة المعلوماتية، دار الكتاب الحديث، القاهرة 2009.

80- معادي أسعد محمد صوالحة، بطاقات الائتمان، النظام القانوني وآليات الحماية الجنائية والأمنية، دار الآفاق المغربية للنشر والتوزيع، الرباط، المملكة المغربية 2008.

81- مناني فراح، العقد الإلكتروني، وسيلة إثبات حديثة في القانون المدني الجزائري، دار الهدى، عين مليلة، الجزائر 2009.

82- مناني فراح، أدلة الإثبات الحديثة في القانون، دار الهدى، عين مليلة، الجزائر 2008.

83- منير محمد الجنبيهي، ممدوح محمد الجنبيهي، تزوير التوقيع الإلكتروني، دار الفكر الجامعي، الإسكندرية، مصر 2006.

84- منير محمد الجنبيهي، ممدوح محمد الجنبيهي، جرائم الانترنت والحاسب الآلي ووسائل مكافحتهما، دار الفكر الجامعي، الإسكندرية، مصر 2006.

85- منير محمد الجنبيهي، ممدوح محمد الجنبيهي، الشركات الإلكترونية، دار الفكر الجامعي، الإسكندرية، مصر 2008.

86- د. نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الاقتصادية، منشورات الحلبي الحقوقية، بيروت، لبنان 2005.

87- د. نزيه عبد المقصود محمد مبروك، المعاملة الضريبية لصفقات التجارة الإلكترونية، دار الفكر الجامعي، الإسكندرية، مصر 2011.

88- نصير الدين حسن أحمد، عناوين مواقع الانترنت، منشورات زين الحقوقية، بيروت، لبنان 2008.

89- نضال سليم برهم، أحكام عقود التجارة الإلكترونية، الطبعة الأولى، الإصدار الثاني، دار الثقافة، عمان، الأردن 2009.

90- د. نعيم مغبغب، حماية برامج الكمبيوتر، الأساليب والثغرات، منشورات الحلبي الحقوقية، بيروت، لبنان 2006.

91- د. نعيم مغبغب، مخاطر المعلوماتية والانترنت على الحياة الخاصة، ط2، منشورات الحلبي الحقوقية، بيروت، لبنان 2008.

92- نهلا عبد القادر المومني، الجرائم المعلوماتية، دار الثقافة للنشر والتوزيع، عمان، الأردن 2008.

93- د. هدى حامد قشقوش، الحماية الجنائية للتجارة الإلكترونية عبر الانترنت، دار النهضة العربية، القاهرة 2000.

94- د. هلالي عبد الله أحمد، حجية المخرجات الكمبيوترية في المواد الجنائية، دار النهضة العربية، القاهرة 1997.

95- وائل أنور بندق، قانون التجارة الإلكترونية، مكتبة الوفاء القانونية، الإسكندرية، مصر 2009.

96- د. يوسف حسن يوسف، التجارة الإلكترونية وأبعادها القانونية الدولية، المصدر القومي للإصدارات القانونية، القاهرة 2011.

97- مكتب الأمم المتحدة المعني بالمخدرات والجريمة UNODC، دليل التعاون الدولي في المسائل الجنائية لمكافحة الإرهاب، مكتب الأمم المتحدة، فينا 2009.

98- مكتب الأمم المتحدة المعني بالمخدرات والجريمة UNODC، دليل المساعدة القانونية المتبادلة وتسليم المجرمين، مكتب الأمم المتحدة، فينا 2013.

ثالثا: أطروحات الدكتوراه

1- أمين أعزان، الحماية الجنائية للتجارة الإلكترونية، دراسة مقارنة، رسالة دكتوراه في الحقوق، جامعة عين (شمس دون ذكر تاريخ المناقشة).

2- إبراهيم بن سطم بن خلف العنزي، التوقيع الإلكتروني وحمايته الجنائية، أطروحة لنيل درجة دكتوراه في الفلسفة، تخصص العلوم الأمنية، جامعة نايف العربية، الرياض 2009.

3- بوراس محمد، الإشهار عن المنتجات والخدمات، دراسة مقارنة، أطروحة دكتوراه في القانون الخاص، جامعة أبي بكر بلقايد، تلمسان 2012/2011.

4- حليمة بن دريس، حماية حقوق الملكية الفكرية في التشريع الجزائري، أطروحة دكتوراه في القانون الخاص، جامعة أبي بكر بلقايد، تلمسان، 2014/2013.

5- خالد بن مبارك القريوي القحطاني، التعاون الأمني الدولي في مواجهة الجريمة المنظمة عبر الوطنية، رسالة دكتوراه في الفلسفة في العلوم الأمنية، كلية الدراسات العليا، جامعة نايف العربية، الرياض2006.

6- رضا أحمد إبراهيم محمود عيد، الأحكام الموضوعية والإجرائية للجرائم الناشئة عن استخدام بطاقة الائتمان، رسالة لنيل درجة دكتوراه في الحقوق، تخصص القانون الجنائي، جامعة عين شمس، مصر (دون ذكر تاريخ المناقشة).

7- سامح أحمد بلتاجي موسى، الجوانب الإجرائية للحماية الجنائية لشبكة الانترنت، رسالة دكتوراه في القانون الجنائي، جامعة الإسكندرية، مصر 2010.

8- سهام لمريني، الخبرة القضائية في المواد الجزائية، أطروحة دكتوراه في القانون، جامعة أبي بكر بلقايد، تلمسان 2014/2013.

9- صالح شنين، الحماية الجنائية للتجارة الإلكترونية، دراسة مقارنة، أطروحة دكتوراه في القانون الخاص، جامعة أبي بكر بلقايد، تلمسان 2013/2012.

10- طارق فوزي الفقي، الجوانب الإجرائية في الجرائم المعلوماتية، رسالة دكتوراه في الحقوق، جامعة المنوفية، مصر 2011.

11- عبد الوهاب مخلوفي، التجارة الإلكترونية عبر الانترنت، أطروحة دكتوراه في الحقوق، تخصص قانون أعمال، جامعة الحاج لخضر، باتنة 2012/2011.

12- فاطمة بحري، الحماية الجنائية للمستهلك، أطروحة دكتوراه في القانون الخاص، جامعة أبي بكر بلقايد، تلمسان 2013/2012.

13- فاطمة زهرة بوعناد، مشروعية الدليل الإلكتروني في مجال الإثبات الجنائي، أطروحة دكتوراه في العلوم، تخصص علوم قانونية، فرع علوم جنائية، جامعة الجيلالي ليابس، سيدي بلعباس 2014/2013.

14- فهد بن سيف بن راشد الحوسني، جرائم التجارة الالكترونية ووسائل مواجهتها مع التطبيق على سلطنة عمان، رسالة مقدمة لنيل درجة دكتوراه في علوم الشرطة، أكاديمية الشرطة، كلية الدراسات العليا، القاهرة 2007.

15- فهد بن محمد النفيعي، الحماية الجنائية للسوق المالي السعودي، رسالة دكتوراه في فلسفة العلوم الأمنية، جامعة نايف العربية للعلوم الأمنية، الرياض 2006.

16- محمد مولود غزيل، معوقات تطبيق التجارة الالكترونية في الجزائر وسبل معالجتها، رسالة لنيل درجة الدكتوراه في العلوم الاقتصادية، تخصص إقتصاد التنمية، جامعة أبي بكر بلقايد، تلمسان 2010.

17- محمد هشام فريجة، دور القضاء الدولي الجنائي في مكافحة الجريمة الدولية، أطروحة دكتوراه علوم في الحقوق، تخصص قانون جنائي، جامعة محمد خيضر، بسكرة 2014/2013.

18- مريم خليفي، الرهانات القانونية للتجارة الإلكترونية، أطروحة دكتوراه في القانون الخاص، جامعة أبي بكر بلقايد، تلمسان 2012/2011.

19- يوسف زروق، حجية وسائل الإثبات الحديثة، أطروحة دكتوراه في القانون الخاص، جامعة أبي بكر بلقايد، تلمسان 2013/2012.

رابعا: مذكرات الماجستير

1- أحمد عبد النور، إشكالية تنفيذ الأحكام الأجنبية، مذكرة ماجستير في القانون الدولي الخاص، جامعة أبي بكر بلقايد، تلمسان2009/.2010

2- أمينة بن عيمور، البطاقات الالكترونية للدفع والقرض والسحب، مذكرة ماجستير في القانون الخاص، تخصص قانون أعمال، جامعة منتوري، قسنطينة، 2004/.2005

3- أمين طعباش، الحماية الجنائية للمعاملات الإلكترونية، مذكرة ماجستير في العلوم القانونية تخصص علم الإجرام والعقاب، جامعة الحاج لخضر باتنة، 2013/2012.

4- حليمة بن دريس، جريمة تقليد العلامات التجارية، مذكرة تخرج لنيل شهادة الماجستير في القانون الخاص، جامعة أبي بكر بلقايد تلمسان، .2008

5- ربيعة فندوشي، الإعلان عبر الانترنت، مذكرة ماجستير في علوم الإعلام والاتصال، جامعة الجزائر 2005/2004.

6- سيدي محمد لبشير، دور الدليل الرقمي في إثبات الجرائم المعلوماتية، رسالة ماجستير في القانون، تخصص التحقيق والبحث الجنائي، جامعة نايف العربية للعلوم الأمنية، الرياض 2010.

7- صالح محمد النويجم : تقويم كفاءة العملية التدريبية في معاهد التدريب الأمنية بمدينة الرياض من وجهة نظر العاملين فيها، رسالة ماجستير في العلوم الإدارية ، جامعة نايف العربية للعلوم الأمنية الرياض 2005.

8- عبد الله ذيب عبد الله محمود، حماية المستهلك في التعاقد الإلكتروني، ماجستير في القانون الخاص، جامعة النجاح، نابلس، فلسطين 2009.

9- فتيحة حواس، حماية المصنفات المنشورة على الانترنت، مذكرة ما جستير، فرع الملكية الفكرية، كلية الحقوق، جامعة الجزائر، 2004.

10- متعب بن عبد الله السند، التعاون الدولي في تنفيذ الأحكام الجنائية وأثره في تحقيق العدالة، رسالة ماجستير في العدالة الجنائية، كلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية، الرياض 2011.

11- محمد بن نصير محمد السرحاني، مهارات التحقيق الجنائي الفني في جرائم الحاسوب و الانترنت، بحث للحصول على درجة الماجستير في قسم العلوم الشرطية، تخصص القيادة الأمنية، جامعة نايف العربية للعلوم الأمنية الرياض 2004.

12- نصيرة خلوي، الحماية القانونية للمستهلك عبر الانترنت، مذكرة لنيل شهادة الماجستير في القانون، فرع المسؤولية المهنية، جامعة مولود معمري تيزي وزو 2013.

13- نعيم سعيداني، آليات البحث و التحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة ماجستير في القانون، تخصص علوم جنائية، جامعة الحاج لخضر، باتنة 2013/2012.

14- ياسر محمد الجبور، تسليم المجرمين أو تقديمهم في الاتفاقيات الدولية والنظام الأساسي للمحكمة الجنائية الدولية، رسالة ماجستير في القانون العام، جامعة الشرق الأوسط، عمان، الأردن 2011.

15- يوسف صغير، الجريمة المرتكبة عبر الانترنت، مذكرة ماجستير في القانون، تخصص القانون الدولي للأعمال، جامعة مولود معمري، تيزي وزو 2013.

خامسا: المقالات والأبحاث العلمية

1- أبو الوفا محمد أبو الوفا، المسؤولية الجنائية عن الاستخدام غير المشروع لبطاقات الائتمان، بحث مقدم إلى مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، المنعقد سنة 2003، كلية الشريعة والقانون، الإمارات، المجلد الخامس.

2- د. أبو الوفا محمد أبو الوفا، جريمة الغش في تداول الأسهم في القانون المقارن والفقه الإسلامي، بحث مقدم إلى مؤتمر أسواق الأوراق المالية والبورصات، كلية الشريعة والقانون. الإمارات العربية المتحدة، 2006.

3- د. أحمد عبد الحليم شاكر علي، دور الإنابة القضائية الدولية في مكافحة الجريمة، مجلة الفكر الشرطي، المجلد17، العدد4، 2008.

4- أحمد فرح، النظام القانوني لمقدمي خدمات الانترنت، مجلة المنارة، المجلد 13، العدد9، الكويت 2007.

5- الأزرق بن عبد الله، أحمد عمراني، نظام المعلوملتية قي القانون الجزائري واقع وآفاق، بحث مقدم إلى المؤتمر السادس لجمعية المكتبات والمعلومات السعودية، الرياض2010.

6- أمجد حمدان الجهني، جرائم بطاقة الدفع الإلكتروني عبر شبكة الانترنت، بحث مقدم إلى مؤتمر المعاملات الإلكترونية المنعقد بالإمارات العربية المتحدة سنة 2006.

7- د. حفيظ الزايدي، الآليات القانونية والإجرائية للحد من آثار الجريمة الإلكترونية على الائتمان المالي، سلسلة ندوات محكمة الاستئناف بالرباط، تأثير الجريمة الإلكترونية على الائتمان المالي، العدد السابع، مطبعة الأمنية، الرباط .2014

8- راضية مشري، الحماية الجزائية للمصنفات الرقمية في ظل قانون حق المؤلف، مجلة التواصل في العلوم الإنسانية والاجتماعية، عدد 34، جوان .2013

9- رامي محمد علوان، المنازعات حول العلامات التجارية وأسماء مواقع الانترنت، مجلة الشريعة والقانون، العدد22، يناير 2005.

10- د. سرحان حسن المعيني، التحقيق في جرائم تقنية المعلومات، الفكر الشرطي، المجلد 20، العدد4، رقم 79، الشارقة، الإمارات العربية المتحدة 2011.

11- عادل عبد الجواد محمد، إجرام الانترنت، مجلة الأمن والحياة، العدد 221، السنة 20، ديسمبر 2000/ يناير .2001

12-عبد الحميد كرود، التسول، النصب والاحتيال عبر الانترنت، مجلة الدركي، العدد16، نوفمبر 2008.

13- عبد المهدي كاظم ناصر، المسؤولية المدنية لوسطاء الانترنت، مجلة القادسية للقانون والعلوم السياسية، العدد الثاني، المجلد الثاني، كانون الأول 2009.

14- د.عدنان إبراهيم سرحان، أسماء النطاق على الشبكة العالمية للمعلوماتية، مجلة الشريعة والقانون، العدد25، يناير 2006.

15- د. علي أحمد صالح المهداوي، أثر خيار الرؤية في حماية المستهلك الإلكتروني، مجلة الشريعة والقانون، العدد 42، أبريل 2010.

16- علي عدنان الفيل، إجراءات التحقيق الابتدائي في الجريمة المعلوماتية، المجلة القانونية التونسية، مركز النشر الجامعي، تونس 2009.

17- د. عمر فاروق الحسيني، لمحة عن جرائم السرقة من حيث اتصالها بنظم المعالجة الآلية للمعلومات، بحث مقدم لكلية الشريعة والقانون، في إطار بحوث مؤتمر القانون والكمبيوتر والانترنت، المنعقد من 1-3 سنة 2000، ط3، المجلد الأول.

18- عيشة خلدون، الطبيعة الخاصة للجريمة الإلكترونية وصورها، مجلة دراسات وأبحاث، العدد 09، جامعة الجلفة، الجزائر 2012.

19- فضيل دليو، الفجوات الرقمية في عصر العولمة، مخبر علم اجتماع الاتصال للبحث والترجمة، جامعة قسنطينة، الجزائر 2010.

20- ليلى الزوين، عرض حول الجرائم الإلكترونية المالية، سلسلة ندوات محكمة الاستئناف بالرباط، تأثير الجريمة الإلكترونية على الائتمان المالي، العدد السابع، مطبعة الأمنية، الرباط 2014.

21- د. محمد الأمين البشري، التحقيق في جرائم الحاسب الآلي، بحث مقدم إلى بحوث مؤتمر القانون والكمبيوتر والانترنت من 1-3 مايو 2000، المجلد الثالث، ط3، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، 2004.

22- محمد بودالي، التوقيع الإلكتروني، مجلة المدرسة الوطنية للإدارة، المجلد 13، العدد26، 2003.

23- أ.د محمد بودالي، الحماية القانونية للمستهلك عن الإشهار الكاذب أو الخادع، مجلة العلوم القانونية والإدارية، العدد 6، سيدي بلعباس 2009.

24- د. محمد حسن عبد الله علي، حماية برامج الحاسب بقانون براءة الاختراع في الولايات المتحدة الأمريكية، مجلة الشريعة والقانون، الإمارات العربية المتحدة، العدد 47، يوليو .2011

25- محمد خليفة، الحماية الجنائية للمستهلك في عقود التجارة الإلكترونية، المجلة التونسية، مركز النشر الجامعي، تونس .2009

26- محمد صبحي نجم، المسؤولية الجزائية عن الاستخدام غير المشروع لبطاقات الائتمان، بحث مقدم لمؤتمر الأعمال الالكترونية بين الشريعة والقانون، المجلد الثالث، الإمارات2004 .

27- أ. د محمد قدري حسن عبد الرحمن، جرائم الاحتيال الإلكتروني، الفكر الشرطي، المجلد 20، العدد4، رقم 79، الشارقة، الإمارات العربية المتحدة 2011.

28- مريم خليفي، العناوين الإلكترونية والعلامات التجارية في مجال التجارة الإلكترونية: روابط ونزاعات، مجلة دراسات وأبحاث، العدد2، جامعة الجلفة، الجزائر.2010

29- مليكة حنان، النظام القانوني للتوقيع الإلكتروني في ضوء قانون التوقيع الإلكتروني السوري رقم 4 الصادر في 2009/02/25، مجلة جامعة دمشق للعلوم القانونية والاقتصادية، المجلد 26، العدد 2، 2010.

30- نهى خالد عيسى، العلامة التجارية المشهورة، دراسة مقارنة، مجلة جامعة بابل للعلوم الإنسانية، المجلد 21، العدد2013/1.

31- أ. د. هدى حامد قشقوش، الحماية الجنائية للتوقيع الإلكتروني، بحث مقدم إلى مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، المجلد الثاني، كلية الشريعة والقانون وغرفة صناعة دبي، 1-12 مايو 2003.

32- د. هشام محمد فريد رستم – الجرائم المعلوماتية " أصول التحقيق الجنائي الفني " - بحث مقدم لمؤتمر القانون والكمبيوتر والإنترنت – كلية الشريعة والقانون بجامعة الإمارات العربية المتحدة في الفترة 1-2000/5/3م المجلد الثاني- الطبعة الثالثة – 2004.

33- القاضي وليد العاكوم، مفهوم وظاهرة الإجرام المعلوماتي، بحث مقدم إلى مؤتمر القانون والكمبيوتر والانترنت، المجلد الأول، الطبعة الثالثة ، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة 2004.

34- - ياسين آيت أحمد، الضوابط القانونية لحماية المستهلك في مجال الإشهار، مجلة العلوم القانونية، العدد الثاني، مطبعة الأمنية، الرباط، المملكة المغربية 2014.

35- د. يوسف شندي، المفهوم القانوني للمستهلك، دراسة تحليلية مقارنة، مجلة الشريعة والقانون، العدد44، أكتوبر 2010.

سادسا: النصوص القانونية

- القانون رقم 03/2000 المؤرخ في 05 غشت 2000 المحدد للقواعد العامة المتعلقة بالبريد والمواصلات السلكية واللاسلكية، ج ر عدد48.

- القانون رقم 09-04 المؤرخ في 05 غشت 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، ج ر عدد47، صادر في 16 غشت 2009.

القانون رقم 15-03 مؤرخ في 01 فبراير 2015، المتعلق بعصرنة العدالة، ج رعدد6، الصادر في 10 فبراير 2015.

القانون رقم 15-04 مؤرخ في 01 فبراير 2015، المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، ج رعدد6، الصادر في 10 فبراير 2015.

- الأمر رقم 66-156 المؤرخ في 08 يونيو 1966 المتضمن قانون العقوبات المعدل والمتمم، إلى غاية القانون رقم 01/14 المؤرخ في 2014/02/04، ج ر07.

- الأمر رقم 66-155 المؤرخ في يونيو 1966 المتضمن قانون الإجراءات الجزائية المعدل والمتمم، إلى غاية الأمر 15-02 المؤرخ في 23 يوليو 2015، ج ر 40.

- الأمر 05/03 المؤرخ في 19 يوليو 2003 المتعلق بحقوق المؤلف والحقوق المجاورة، ج ر العدد 44، الصادر في 23 يوليو 2003.

- المرسوم الرئاسي رقم 94-181 المؤرخ في 27 يونيو 1994،المتضمن التصديق على اتفاقية التعاون القانوني والقضائي بين دول اتحاد المغرب العربي الموقعة بليبيا عام 1991 ج رعدد43 الصادر في 03 يوليو 1994.

- المرسوم الرئاسي رقم 01-47 المؤرخ في 11 فبراير 2001، المتعلق بالتصديق على اتفاقية الرياض للتعاون القضائي التي اعتمدها مجلس وزراء العدل العرب في دورته الأولى بالقرار رقم 01 في1983/4/6، ج رالعدد11 الصادر في 12 فبراير 2001.

- المرسوم الرئاسي رقم 13-123 المؤرخ في 2013/04/03 يتضمن التصديق على معاهدة المنظمة العالمية للملكية الفكرية (الويبو) بشأن حق المؤلف، المعتمدة بجنيف بتاريخ 1996/12/30، ج ر عدد27 صادر في 2013/05/22.

- المرسوم الرئاسي رقم 14-252 مؤرخ في 08 سبتمبر 2014، المتضمن التصديق على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، المحررة بالقاهرة بتاريخ 21 ديسمبر 2010، ج رعدد 57، صادر في 28 سبتمبر 2014.

- المرسوم الرئاسي رقم 15-261 مؤرخ في 08 أكتوبر 2015، المحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج ر عدد 53، صادر في 08 أكتوبر 2015.

- المرسوم التنفيذي رقم 98-257 مؤرخ في 25 غشت 1998، يضبط ويحدد شروط وكيفيات إقامة خدمات "انترنت" واستغلالها، المعدل بموجب المرسوم التنفيذي رقم 2000-307، المؤرخ في 2000/10/14، ج ر63 لعام 1998.

- المرسوم التنفيذي رقم 07-162 المؤرخ في 30 مايو 2007، المعدل والمتمم للمرسوم التنفيذي رقم 01-123 المؤرخ في 09 مايو 2001، والمتعلق بنظام الاستغلال المطبق على كل نوع من الشبكات بما فيها اللاسلكية الكهربائية وعلى مختلف خدمات المواصلات السلكية واللاسلكية. ج ر العدد37 الصادر في 07 يونيو 2007.

- إتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية بتاريخ 15-11-2000.

- إتفاقية بودابست الموقعة في 23-11-2001 والمتعلقة بالجرائم الإلكترونية.

- قانون الأونسترال النموذجي بشأن التجارة الإلكترونية سنة 1996.

- قانون الأونسترال النموذجي بشأن التوقيع الإلكتروني سنة 2001.

- القانون العربي الاسترشادي بشأن المعاملات والتجارة الإلكترونية، المعتمد بقرار من وزراء العدل العرب، رقم 812/د25، بتاريخ 2009/11/19.

– القانون العربي الاسترشادي للإثبات بالتقنيات الحديثة الذي اعتمده مجلس وزراء العدل العرب بقرار رقم 771/د24 في 2008/11/27.

المراجع باللغة الفرنسية.

1- *Les ouvrages.*

1- Aboudramane Ouattara, la preuve électronique, étude de droit comparé Afrique Europe Canada, presses universitaires d'aix Marseille, 2011.

2- Béatrice Clément et autres, fiches de droit pénal spécial, ellipses édition, Paris 2012.

3- Celine Castets-Renard, droit de l'internet, montchrestien, Lextenso édition, Paris 2010.

4- Christiane Féral-Schuhl, cyberdroit, le droit à l'épreuve de l'internet, 6ème édition, Praxis Dalloz, Paris 2011/2012.

5- Christophe Caron, droit d'auteur et droit voisins, 3ème édition, lexisNexis, Paris 2013.

6- Guillaume Blanc- Jouvan, droit de la propriété intellectuelle, Vuibert, Paris 2011.

7- Jacques Larrieu, droit de l'internet, 2ème édition,ellipses édition, Paris 2010.

8- Jacques Leroy, procédure pénale, librairie générale de droit et de jurisprudence, Lextenso édition, paris cedex 2009.

9- Jean Larguier et autres, droit pénal spécial, 14 ème édition, Dalloz, Paris 2008.

10- Jean-Michel Bruguière, droit des propriétés intellectuelles, 2ème édition,ellipses édition, Paris 2011.

11- Jean Stoufflet, instruments de paimentt et de crédit, 8 ème édition lexisNexis, Paris 2012.

12- Marie-Christine Sordino, droit pénal des affaires, bréal, Paris 2010.

13- Patrick Klob, Laurence Leturmy, droit pénal général, 5ème édition, Gualino lextenso éditions, Paris 2010.

14- Nathalie Dreyfus, marques et internet, Lamy, Paris 2011.

15- RomainV.Gola, droit du commerce électronique, Gualino lextenso éditions, Paris 2013.

16- Renaud Salomon, droit pénal des affaires, lexisNexis, Litec, Paris 2009.

17- Roseline Letteron, libertés publiques, 9 ème édition, Dalloz, Paris 2012.

18- Santiago Cavanillas et autres, commerce électronique le temps des certitudes, edition delta, Beyrouth, Liban 2001.

19- Tayeb Belloula, droit pénal des affaires et des sociétés commerciales, Berti éditions, Alger 2011.

20- Wilfrid jeandidier, droit pénal des affaires, 6ème édition, Dalloz, Paris 2005.

2- *Articles, theses universitaires. et sites internet*

1-Chloé Torres, renforcement des contrôles de la CNIL dans le cadre de la proposition de la loi du 06 novembre 2009, Gazette du palais1, Janvier Février, Paris 2010.

2- Emmanuel Dreyer, nouvelle responsabilité du producteur sur internet, Recueil Dalloz, 17 janvier 2013.

3- Eric Barbry, le droit de l'internet est devenu au fil des années un droit spécial? Gazette du palais5, septembre octobre 2010.

4- Mathieu Prud'homme, l'usurpation d'identité numérique: bientôt un nouveau délit, Gazette du palais 2, Mars Avril 2010.

5- Pierre Sirinelli, la responsabilité des prestataires de l'internet, conférence de transaction électronique, EUA,2009.

6- Delphine Galan, la protection de la création olfactive par le droit de la propriété intellectuelle, thèse Pour obtenir le grade de docteur de l'université d'AVIGNON et des pays de VAUCLUSE, Discipline : Droit privé, faculté de droit, france2008.

7- Mme kheira Dari Bekara, protection des données personnelles coté utilisateur dans le e commerce, thèse de doctorat conjoint Télecom Sud Paris et l'université Pierre et Marie Curie, Paris 2012, p42-45.

8- Régis Buchillet, la responsabilité des prestataires techniques de l'internet, DEA en droit de l'économie, mention droit international, université de Bourgogne, France 2001/2002.

9- Virginie Etienne, le developpement de la signature électronique, Master2, droit des affaires, université Paris nord 13,2011/2012.

10-www.légalis.net

11-www.légifrance.gouv.fr

3- les lois

Code pénal français (Dernière modification du texte le 28 mars 2015 - Document généré le 08 mai 2015 - Copyright (C) 2007-2008 Legifrance)

Code de procédure pénal français (Dernière modification du texte le 19 avril 2015 - Document généré le 30 avril 2015 - Copyright (C) 2007-2008 Legifrance)

Code de la propriété intellectuelle français(Dernière modification du texte le 19 avril 2015 - Document généré le 30 avril 2015 - Copyright (C) 2007-2008 Legifrance).

Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique.

Loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel

et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

DIRECTIVE 1999/93/CE DU PARLEMENT EUROPÉEN ET DU CONSEIL du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques.

DIRECTIVE 2001/29/CE DU PARLEMENT EUROPÉEN ET DU CONSEILdu 22 mai 2001sur l'harmonisation de certains aspects du droit d'auteur et des droits voisins dans la société del'information.

DIRECTIVE 2000/31/CE DU PARLEMENT EUROPE´ EN ET DU CONSEIL du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment ducommerce électronique, dans le marché intérieur («directive sur le commerce électronique»)

DIRECTIVE 2002/58/CE DU PARLEMENT EUROPÉEN ET DU CONSEILdu 12 juillet 2002concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques).

الفهرس

مقدمة. ---------- 1

الفصل التمهيدي: التجارة الإلكترونية والجرائم المعلوماتية---------- 15

المبحث الأول: ماهية التجارة الإلكترونية ---------- 15

المطلب الأول: مفهوم التجارة الالكترونية ومميزاتها. ---------- 15

الفرع الأول:مفهوم التجارة لإلكترونية.---------- 15

أولا: تعريف التجارة الإلكترونية---------- 15

ثانيا: مراحل تطور وظهور التجارة الالكترونية ---------- 22

الفرع الثاني: مميزات التجارة الالكترونية ---------- 23

أولا: أنواع وخصائص التجارة الالكترونية---------- 23

ثانيا: وسائل التجارة الالكترونية.---------- 26

المطلب الثاني: واقع وآفاق التجارة الالكترونية ---------- 33

الفرع الأول:عوائق و تحديات التجارة الإلكترونية---------- 33

أولا: عوائق التجارة الالكترونية. ---------- 33

ثانيا: دول العالم الثالث والفجوة الرقمية ---------- 35

الفرع الثاني: واقع وآفاق التجارة الالكترونية بالجزائر.---------- 38

أولا : واقع التجارة الالكترونية في الجزائر. ---------- 38

ثانيا: آفاق التجارة الالكترونية في الجزائر. ---------- 40

المبحث الثاني: جرائم ومجرمو المعلوماتية. ---------- 41

المطلب الأول: جرائم المعلوماتية. ---------- 41

الفرع الأول: مفهوم وخصائص جرائم المعلوماتية . ---------- 42

أولا: مفهوم جرائم المعلوماتية. ---------- 42

ثانيا: خصائص جرائم المعلوماتية. ---------- 44

الفرع الثاني: أنواع الجرائم المعلوماتية وأضرارها.---------- 47

أولا: أنواع الجرائم المعلوماتية. ---------- 47

ثانيا: أضرار الجرائم المعلوماتية. ---------- 51

المطلب الثاني: مجرمو المعلوماتية. ---------- 53

الفرع الأول: تعريف المجرم المعلوماتي وصفاته. ---------- 53

الفرع الثاني:أصناف مجرمي المعلوماتية ودوافعهم ---------- 55

الباب الأول: الجرائم الواقعة على التجارة الإلكترونية. ---------- 59

الفصل الأول: الحماية الجزائية لمواقع التجارة لإلكترونية على الانترنت ومحتوياتها. ---------- 59

المبحث الأول: تجريم الاعتداء على نظم المعالجة الآلية للمعطيات. ---------- 59

المطلب الأول: الأحكام المشتركة بين جرائم الاعتداء على نظم المعالجة الآلية للمعطيات. --------- 63

الفرع الأول: مفهوم نظام المعالجة الآلية للمعطيات. ---------- 63

الفرع الثاني: المصلحة المحمية في جرائم نظم المعلومات. ---------- 65

الفرع الثالث: العقوبات التكميلية. ---------- 66

الفرع الرابع: المبادئ المشتركة بين جرائم الاعتداء على أنظمة المعالجة الآلية للمعطيات. --------- 69

أولا: مبدأ مسؤولية الشخص المعنوي. ---------- 70

ثانيا: مبدأ المعاقبة على الشروع. ---------- 71

ثالثا: مبدأ المعاقبة على الأعمال التحضيرية المادية الجماعية. ---------- 71

المطلب الثاني: جريمة الدخول أو البقاء غير المشروع في نظام المعالجة الآلية للمعطيات. ---------- 74

الفرع الأول: جريمة الدخول أو البقاء البسيطة. ---------- 75

أولا: الركن المادي لجريمة الدخول أو البقاء البسيطة. ---------- 75

ثانيا: الركن المعنوي لجريمة الدخول أو البقاء البسيطة. ---------- 79

الفرع الثاني: جريمة الدخول أو البقاء المشددة. ---------- 81

المطلب الثالث: إعاقة أو التسبب في تحريف تشغيل نظام معالجةمعطيات التجارة الالكترونية. ------- 83

الفرع الأول: الركن المادي. ---------- 84

أولا: التعطيل أو الإعاقة. ---------- 84

ثانيا: الإفساد أو التعييب. ---------- 86

الفرع الثاني: الركن المعنوي. ---------- 86

المطلب الرابع: جريمة التلاعب في معطيات الحاسب الآلي. ---------- 88

الفرع الأول: الركن المادي. ---------- 88

أولا: الإدخال. ---------- 89

ثانيا: المحو أو الإزالة. ---------- 89

ثالثا: التعديل. ---------- 90

الفرع الثاني: الركن المعنوي. ---------- 90

المطلب الخامس:جريمة التعامل في معطيات غير مشروعة ---------- 92

الفرع الأول: الركن المادي لجريمة التعامل في معطيات غير مشروعة ---------- 93

الفرع الثاني: الركن المعنوي لجريمة التعامل في معطيات غير مشروعة ---------- 96

المبحث الثاني: الحماية الجزائية لحقوق الملكية الفكرية المتعلقة بالتجارة الالكترونية. ---------- *98*
المطلب الأول: الحماية الجزائية لمحتويات مواقع التجارة الالكترونية في ضوء قوانين حماية الملكية الفكرية. -- 98
الفرع الأول: علاقة التجارة الالكترونية بالملكية الفكرية. ---------- 98
الفرع الثاني: الحماية التي توفرها قوانين حماية الملكية الفكرية. ---------- 100
الفرع الثالث: جنحة التقليد والجنح الشبيهة بها. ---------- 102
أولا: جريمة التقليد. ---------- 103
ثانيا: الجرائم الملحقة بجرائم التقليد. ---------- 113
المطلب الثاني: حماية أسماء النطاق على شبكة الانترنت. ---------- 116
الفرع الأول: ماهية أسماء النطاق. ---------- 116
أولا: مفهوم أسماء النطاق. ---------- 116
ثانيا: الطبيعة القانونية لأسماء النطاق. ---------- 118
ثالثا: أنواع أسماء النطاق. ---------- 120
الفرع الثاني:النزاعات القانونية لأسماء النطاق ---------- 121
أولا: التنازع بين اسم النطاق والعلامة التجارية. ---------- 122
ثانيا: التنازع بين اسم النطاق وغيره من مواضيع القانون. ---------- 125
ثالثا: تسوية المنازعات بين مسجلي أسماء النطاق ومالكي العلامات التجارية ---------- 126
الفصل الثاني: الحماية الجزائية للمستهلك في مجال التجارة الإلكترونية. ---------- *135*
المبحث الأول: الحماية الجزائية للمستهلك الإلكتروني من جرائم الأموال. ---------- *136*
المطلب الأول: الحماية الجزائية للمستهلك الإلكتروني من جرائم الأموال التقليدية. ---------- 136
الفرع الأول: السرقة والتجارة الإلكترونية. ---------- 136
أولا: محل السرقة في التجارة الإلكترونية. ---------- 137
ثانيا: صور وأركان السرقة في مجال التجارة الإلكترونية. ---------- 139
الفرع الثاني: جريمة النصب والاحتيال. ---------- 141
أولا: مفهوم جريمة النصب. ---------- 141
ثانيا: النصب في مجال التجارة الإلكترونية. ---------- 143
الفرع الثالث: جريمة التزوير. ---------- 149
أولا: مفهوم جريمة التزوير. ---------- 149
ثانيا: جريمة التزوير والتجارة الإلكترونية. ---------- 151
الفرع الرابع:جريمة خيانة الأمانة. ---------- 154
أولا: مفهوم جريمة خيانة الأمانة. ---------- 155
ثانيا: جريمة خيانة الأمانة والتجارة الإلكترونية. ---------- 156

الفرع الخامس: جريمة الإتلاف. ---------- 157
أولا: أركان جريمة الإتلاف.---------- 157
ثانيا: الإتلاف والتجارة الإلكترونية---------- 159
المطلب الثاني: الحماية الجزائية للمستهلك الإلكتروني من الجرائم المستحدثة ---------- 163
الفرع الأول: حماية المستهلك من الإعلانات التجارية الإلكترونية الكاذبة أو الخادعة. ---- 163
أولا: التنظيم القانوني للإعلانات التجارية الإلكترونية.---------- 164
ثانيا: الحماية الجزائية للمستهلك من الإعلانات التجارية الإلكترونية الكاذبة أو الخادعة. ----- 168
الفرع الثاني: الحماية الجزائية لبطاقات الائتمان. ---------- 174
أولا: الاستخدام غير المشروع لبطاقة الائتمان من قبل حاملها. ---------- 176
ثانيا: الاستخدام غير المشروع لبطاقة الائتمان من قبل الغير. ---------- 188
الفرع الثالث: الحماية الجزائية للتوقيع الإلكتروني ---------- 193
أولا: ماهية التوقيع الإلكتروني. ---------- 193
ثانيا: صور الاعتداءات الواقعة على التوقيع الالكتروني. ---------- 205
المبحث الثاني: الحماية الجزائية للحق في الخصوصية للمستهلك الإلكتروني. ---------- *216*
المطلب الأول: الحماية الجزائية للبيانات الشخصية. ---------- 217
الفرع الأول: الحماية الجزائية للبيانات الشخصية في القانون الفرنسي ---------- 219
أولا: جريمة عدم اتخاذ الإجراءات الأولية لإجراء معالجة البيانات.---------- 220
ثانيا: جريمة عدم اتخاذ الاحتياطات اللازمة لحماية البيانات المعالجة. ---------- 222
ثالثا: جريمة المعالجة غير المشروعة للبيانات. ---------- 223
رابعا: جريمة تسجيل وحفظ بيانات شخصية أو بيانات تتعلق بالماضي لأشخاص مصنفين.---- 224
خامسا: جريمة حفظ بيانات شخصية خارج الوقت المصرح به وفقا للطلب أو الإعلان السابق. - 225
سادسا: جريمة تغيير الغرض المحدد لجمع البيانات الاسمية.---------- 225
سابعا: جريمة الإفشاء غير المشروع للبيانات الاسمية ---------- 226
ثامنا: جريمة التنصت على المراسلات. ---------- 228
تاسعا: إعاقة مهام اللجنة الوطنية للمعلوماتية والحريات ---------- 229
الفرع الثاني: الحماية الجزائية للبيانات الشخصية في بعض التشريعات العربية ---------- 230
أولا: الحماية الجزائية للبيانات الشخصية في التشريع المصري---------- 230
ثانيا: الحماية الجزائية للبيانات الشخصية في التشريع التونسي ---------- 231
ثالثا: الحماية الجزائية للبيانات الشخصية في التشريع الجزائري ---------- 233
المطلب لثاني: المسؤولية الجزائية لمقدمي الخدمات الوسيطة عبر الانترنت. ---------- 236
الفرع الأول: الطبيعة القانونية لخدمات الإنترنت وصفة مقدميها. ---------- 238

أولا : خدمات الإيواء. ---------- 238
ثانيا: خدمات توريد المعلومات ---------- 241
ثالثا: خدمات النقل المادي للمعلومات. ---------- 242
رابعا: خدمات الوصول. ---------- 243
الفرع الثاني: التزامات مقدمي خدمات الإنترنت. ---------- 244
أولا: التزامات مقدمي الخدمة المعلوماتية. ---------- 245
ثانيا: التزامات مقدمي الخدمة الفنية.---------- 252
الفرع الثالث: مسؤولية مقدمي خدمات الإنترنت عما يحدث من مخالفات عبر الشبكة. ------- 256
أولا: المسؤولية الجزائية لمتعهد الوصول ---------- 257
ثانيا المسؤولية الجزائية لمتعهد الإيواء---------- 259
ثالثا: المسؤولية الجزائية للمنتج---------- 262
رابعا: المسؤولية الجزائية لناقل المعلومات ---------- 265
خامسا: المسؤولية الجزائية لمتعهد الخدمات ---------- 266
سادسا: المسؤولية الجزائية لمورد المعلومات---------- 267
سابعا:المسؤولية الجزائية لمؤلف الرسالة ---------- 267

الباب الثاني: القواعد الإجرائية المتعلقة بالتجارة الإلكترونية. ---------- 270

الفصل الأول: الحماية الإجرائية الوطنية للتجارة الإلكترونية.---------- 271

المبحث الأول: الحماية الجزائية للتجارة الإلكترونية من خلال الإجراءات الجزائية السابقة على المحاكمة.------ 271
المطلب الأول: الضبط في مجال الجرائم المتصلة بالتجارة الإلكترونية. ---------- 272
الفرع الأول: الضبط الإداري ودوره في الوقاية من الجرائم الواقعة على التجارة الإلكترونية.------- 272
أولا: مفهوم الضبط الإداري.---------- 272
ثانيا: الضبط الإداري الاقتصادي ودوره في حماية التجارة الإلكترونية. ---------- 274
الفرع الثاني: الضبط القضائي ودوره في التصدي للجرائم الواقعة على التجارة الإلكترونية. ------ 275
الفرع الثالث: دور شرطة الانترنت في حماية التجارة الإلكترونية ---------- 278
المطلب الثاني: التحقيق في الجرائم الواقعة على التجارة الإلكترونية.---------- 283
الفرع الأول: خصائص التحقيق في الجرائم الواقعة على التجارة الإلكترونية. ---------- 283
أولا: مفهوم التحقيق في الجرائم الواقعة على التجارة الإلكترونية. ---------- 283
ثانيا: صعوبة كشف الجرائم الواقعة على التجارة الإلكترونية. ---------- 284
ثالثا: سير التحقيق في الجرائم الواقعة على التجارة الإلكترونية. ---------- 288
الفرع الثاني: إجراءات التحقيق في الجرائم الواقعة على التجارة الإلكترونية. ---------- 290

أولا: الإجراءات التقليدية في تحقيق الجرائم الإلكترونية. ---------- 290
ثانيا: الإجراءات المستحدثة في تحقيق الجرائم الإلكترونية. ---------- 313
المبحث الثاني: الحماية الجزائية للتجارة الإلكترونية في مرحلة المحاكمة.---------- 323
المطلب الأول: تحديد المحكمة المختصة في الجرائم الواقعة على التجارة الإلكترونية. ---------- 323
الفرع الأول: الموقف الفقهي من تنازع الاختصاص الجنائي. ---------- 324
أولا : مذهب السلوك أو النشاط الإجرامي بوصفه معيارا لتحديد مكان وقوع الجريمة. ------ 324
ثانيا : مذهب مكان تحقق النتيجة كمعيار لتحديد الاختصاص. ---------- 325
ثالثا: المذهب المختلط. ---------- 326
الفرع الثاني: الموقف التشريعي والقضائي من تنازع الاختصاص الجزائي الدولي. -------- 327
أولا: مبدأ إقليمية النص الجزائي. ---------- 328
ثانيا: مبدأ شخصية النص الجزائي. ---------- 331
ثالثا: مبدأ عينية النصوص الجزائية. ---------- 332
رابعا: مبدأ الاختصاص العالمي. ---------- 333
الفرع الثالث: الاختصاص الجزائي الداخلي بالنسبة لجرائم التجارة الإلكترونية --------- 335
المطلب الثاني: سلطة المحكمة المختصة في قبول وتقدير الدليل في مجال التجارة الإلكترونية. ------- 338
الفرع الأول: سلطة القاضي الجزائي في قبول الدليل الإلكتروني. ---------- 338
أولا: أساس قبول الدليل الإلكتروني في الإثبات الجزائي.---------- 338
ثانيا: خصائص ومميزات الدليل الإلكتروني ---------- 340
ثالثا: القيمة القانونية للدليل الإلكتروني---------- 342
الفرع ثاني: سلطة القاضي الجزائي في تقدير الدليل الإلكتروني. ---------- 344
أولا: نطاق سلطة القاضي الجزائي في تقدير الدليل الالكتروني. ---------- 344
ثانيا: الضوابط التي تحكم اقتناع القاضي الجزائي بالدليل الإلكتروني. ---------- 345
الفصل الثاني: التعاون الدولي لمكافحة الجرائم الواقعة على التجارة الإلكترونية. ---------- *348*
المبحث الأول: ضرورة التعاون الدولي في مجال مكافحة الجرائم الواقعة على التجارة الإلكترونية. ------- *350*
المطلب الأول: التعاون القضائي في مجال مكافحة الجرائم الواقعة على التجارة الإلكترونية. -------- 351
الفرع الأول: المساعدة القضائية الدولية.---------- 351
أولا: طبيعة المساعدة القضائية الدولية.---------- 351
ثانيا: صور المساعدة القضائية الدولية.---------- 354
ثالثا: طلب المساعدة القضائية. ---------- 356
الفرع الثاني: الإنابة القضائية الدولية. ---------- 357
أولا: تعريف الإنابة القضائية الدولية.---------- 357

ثانيا: إجراءات طلب الإنابة القضائية الدولية. ---------- 358
الفرع الثالث: نقل الإجراءات الجزائية. ---------- 360
الفرع الرابع: الاعتراف بتنفيذ الأحكام الجنائية. ---------- 362
المطلب الثاني: تسليم المجرمين.---------- 365
الفرع الأول: تعريف تسليم المجرمين وصوره. ---------- 365
أولا: تعريف تسليم المجرمين. ---------- 366
ثانيا: صور وشروط تسليم المجرمين.---------- 367
الفرع الثاني: تسليم المجرمين في القانون الجزائري ---------- 374
المطلب الثالث: التعاون الدولي الأمني في مكافحة الجرائم الواقعة على التجارة الإلكترونية. -------- 374
الفرع الأول: تعريف التعاون الدولي الأمني. ---------- 374
الفرع الثاني: الجهود الدولية في مجال التعاون الأمني.---------- 377
أولا: جهود المنظمة الدولية للشرطة الجنائية. ---------- 377
ثانيا:جهود جهاز الشرطة الأوربية. ---------- 381
ثالثا: دور اليوروجست في الكشف عن الجرائم الإلكترونية. ---------- 382
رابعا: المدعي العام الأوربي:---------- 382
خامسا: دور مجلس وزراء الداخلية العرب.---------- 383
سادسا: دور المنظمة الدولية لضباط الجرائم المالية. ---------- 383
سابعا: التعاون من خلال نظام "شنجين" للمعلومات. ---------- 383
الفرع الثالث: التعاون الدولي في مجال التدريب على مواجهة الجرائم الإلكترونية. ---------- 384
أولا: التدريب وأهميته في مجال مكافحة الجرائم الإلكترونية.---------- 385
ثانيا: مظاهر التعاون الدولي في مجال تدريب رجال العدالة الجزائية. ---------- 388
المبحث الثاني: صعوبات التعاون الدولي وسبل التغلب عليها.---------- 392
المطلب الأول: صعوبات التعاون الدولي في مجال مكافحة الجرائم الواقعة على التجارة الإلكترونية. ---- 392
الفرع الأول: تنازع الاختصاص القضائي. ---------- 393
الفرع الثاني: ازدواجية التجريم. ---------- 395
الفرع الثالث: قصور بعض التشريعات الوطنية. ---------- 396
الفرع الرابع: الاعتبارات السياسية والفنية. ---------- 397
المطلب الثاني: الجهود المبذولة للتغلب على معوقات التعاون الدولي.---------- 400
الفرع الأول: الجهود الوطنية للتغلب على معوقات التعاون الدولي. ---------- 400
الفرع الثاني: الجهود الدولية للتغلب على معوقات التعاون الدولي. ---------- 402

خاتمة ---------- 407
قائمة المراجع ---------- 418
المراجع باللغة العربية---------- 418
المراجع باللغة الفرنسية. ---------- 439