الجمهورية التونسية

محكمة التعقيب

مكتب الرئيس الأول

الجرائم الالكترونية الواقعة على الأموال في القانون التونسي

لقد مهدت الثورة الصناعية في منتصف القرن الماضي لبروز ثورة جديدة وهي ثورة المعلومات والتي كانت وراء ما يطلق عليه "صناعة المعلوماتية". حيث ظهرت منافذ استثمارية جديدة تمثلت في مؤسسات ومشروعات فردية، منها ما يهتم بتصنيع الحاسبات ومنها ما يتصدى لإعداد البرامج اللازمة لمعالجة المعلومات آليا وأخرى لبيع هذه أو تلك أو التعامل فيها بصفة عامة. ومع ظهور تلك الصناعة واستخداماتها المتعددة نشأت علاقات قانونية جديدة في مجال فروع القانون المختلفة ومنها القانون الجزائي[1].

ورغم أهميتها، فإن الثورة المعلوماتية أو الرقمية مثل كل تطور جديد تحمل في طياتها جانبا مظلما يتجسد في مجال القانون الجزائي بظهور "المجرم المعلوماتي " و" " الجريمة المعلوماتية " أو ظاهرة " الإجرام المعلوماتي " بصفة عامة[2].

تعرف المعلوماتيّة بعلم المعلومات أو تكنولوجيا المعلومات، أي المعلومة الخاضعة للمعالجة الإلكترونيّة، وهي مشتقّة من كلمة المعلومة information من ناحية، ومن كلمة الأوتوماتيك automatique من ناحية أخرى. وعرّفها القانون الفرنسي " بعلم المعالجة العقلانيّة، لاسيّما بواسطة الآلات الأوتوماتيكيّة للمعلومة التّي تعتبر مرتكزا للمعارف الإنسانيّة ولوسائل الاتّصال في المجال التّقني والاقتصادي والاجتماعي "[3]. ويبدو هذا المفهوم واسعا بحكم ارتباطه الشّديد بمدى التّقدّم الحاصل في مجال المعالجة والأنظمة الإلكترونيّة، والتّطوّر السّريع الذّي

[1] الجدير بالملاحظة أن طغيان المنظومات الإعلامية على الحياة المعاصرة وتأثيرها في العلاقات الاقتصادية بمختلف أشكالها وميادينها يجعل من البحث عن طرق حمايتها من الانحراف بها إلى المسار السلبي أمرا ملحا ضرورة أن الروابط الاقتصادية تحتكم إلى أطر وقواعد ومبادئ قانونية تنظمها ويكون من الأوكد إخضاع هذه المبتكرات التكنولوجية الى تلك القواعد أو خلق قواعد أخرى تتلاءم مع خصوصياتها. فلقد أصبح من المألوف أن كل إكتشاف علمي جديد يحمل معه مصاعب تطويعه وتنظيمه بالقواعد القانونية الساندة حتى لا يظل وسيلة تهديم عوض أن يكون أداة تطوير وتجديد.

[2] J. PRADEL, les infractions relatives à l'informatique, R.I.D.P. 2. 1999 , pp. 815-828

[3] Xavier Linand de Beffonds et A. HOLLANDE, Droit de l'informatique et de la télématique. 2éme édit., J.DELMAS et Cie, 1990, pp. 99 et ss.

يشهده هذا القطاع. والمعلوماتيّة في نهاية الأمر لا تخرج عن استعمالات الكمبيوتر أو الآلة الحاسبة وما تفرضه من تقنيّات حتّمتها مظاهر تقدّم هذا المجال وما تفرزه من خدمات عبر المعالجة الآلية للبيانات[4].

وتكون هذه المعالجة محلّ نظام متكامل، يعرف بنظام المعالجة الآليّة للبيانات إذا توفّرت عناصر هذا النّظام: - système de traitement automatisé des données-، وهو مجموعة وحدات معالجة وذاكرة وبرمجيّات ومعطيات وروابط، منظّمة بهدف تحقيق نتيجة معيّنة، وعادة ما يكون هذا النّظام محميّا ومؤمّنا، سواء باستعمال كلمة السّر أو كلمة العبور أو منظومة التّشفير أو أيّ طريقة فنيّة أخرى. معنى ذلك أنّ تتناسق العناصر من أجل تحقيق المعالجة وحمايتها. أو هو " كلّ وحدة مستقلّة أو مجموعة من الوحدات المترابطة والمتقاربة والتّي يضمن إحداها أو جميعها، تنفيذا لبرنامج محدّد، المعالجة الإلكترونيّة، أو عدّة أعمال أخرى"[5].

ويخرج من مفهوم المعالجة مفهوم البيانات أو المعطيات الإلكترونيّة، أي المعلومة في شكلها الإلكتروني بعد أن خضعت لإجراء المعالجة. وتفهم المعطيات الإلكترونيّة على أنّها مفهوم مجرّد، فتأتي خالصة عن دلالاتها ومقاصدها. وإذا أردت أن تسند إلى هذه المعطيات بعدها الفلسفي والاقتصادي والاجتماعي والسّياسي، وغير ذلك من التّعابير الثّقافيّة، فنقول عندئذ بالمحتوى المعلوماتي. فالمعطيات الإلكترونيّة هو مفهوم مجرّد غير واعي، والمحتوى هو مفهوم واقعي وذو مقاصد متعدّدة.

الجرائم الالكترونية تربط أشد الارتباط بالمعلوماتية ويطلق عليها " غش المعلوماتية ". ويقصد بها كل سلوك غير مشروع يتعلق بالمعلومات المعالجة ونقلها[6].

---

[4] غازي عبد الرحمن هيان الرشيد، الحماية القانونية من جرائم المعلوماتية(الحاسوب الانترنت)، أطروحة دكتوراه في القانون، الجامعة الإسلامية في لبنان، كلية الحقوق، 2004، ص.90 وما بعد.
محمد علي العريان، الجرائم المعلوماتية، الإسكندرية، 2004، ص.43.
مصطفى محمد موسى، أساليب إجرامية بالتقنية الرقمية(ماهيتها،مكافحتها)، دار الكتب القانونية، مصر2005، ص.50 وما بعد.
عبدالله عبد الكريم عبدالله، جرائم المعلوماتية والانترنت(الجرائم الالكترونية)، منشورات الحلبي الحقوقية، بيروت، الطبعة الأولى2007، ص.15.

[5] سامي القلال ، النزاع حول البرامج المعلوماتية في الجمهورية التونسية ، م ق.ت ،عدد10 ، شهر ديسمبر1996. ص46.

[6] تعبير "غش المعلوماتية " وان استقام استخدامه في مجال علم الإجرام للتعبير عن المظاهر الإجرامية المختلفة التي يتصور إرتباطها بالمعلوماتية ، إلا أنه في مجال القانون الجنائي يعد تعبيرا غامضا ويمكن أن يحل محله " جرائم المعلوماتية" .

وهذه الجرائم يمكن تصورها من زاويتين بحسب دورها في التجريم. فمن الزاوية الأولى تكون المعلوماتية **موضوعا للاعتداء** وهي من الزاوية الثانية **أداة أو وسيلة للإعتداء**[7].

فإذا نظرنا إليها من الزاوية الأولى نلاحظ أن الجاني يتجه قصده الى الإعتداء على الشيء أو المال محلا أو موضوعا لها. أما إذا نظرنا لجرائم المعلوماتية من الزاوية الثانية نلاحظ أن الجاني يستخدم المعلوماتية لتنفيذ جرائمه سواء ما تعلق منها بجرائم الإعتداء على الأموال مثل التحيل و السرقة وخيانة الأمانة بخصوص بطاقات السحب ، أو بطاقات الدفع أو التحويل البنكي[8].

فجرائم السطو على ارقام بطاقات الائتمان والتحويل الإلكتروني غير المشروع للأموال تتمثل في استخدام البطاقات الائتمانية من خلال شبكة الانترنت واكبه ظهور الكثير من المتسللين للسطو عليها, باعتبارها نقودا الكترونية, خاصة من جهة ان الاستيلاء على بطاقات الائتمان امرا ليس بالصعوبة بمكان, فلصوص بطاقات الائتمان مثلا يستطيعون الان سرقة مئات الألوف من ارقام البطاقات في يوم واحد من خلال شبكة الانترنت ومن ثم بيع هذه المعلومات للأخرين[9].

تتم عملية التحويل الالكتروني غير المشروع للأموال من خلال الحصول على كلمة السر المدرجة في ملفات أنظمة الكمبيوتر الخاصة بالمجني عليه. مما يسمح للجاني بالتوغل في النظام المعلوماتي وعادة ما يكون هؤلاء من العاملين على ادخال البيانات في ذاكرة الجهاز أو من قبل المتواجدين على شبكة أثناء عملية تبادل البيانات ، وتتم عملية التحويل الإلكتروني غير المشروع للأموال بعدة طرق[10].

---

[7] R. GHASSIN, Le droit pétral de l'informatique , D, 1986, 5éme cahier, chron,pp. 35-42 ;

JDEVEZE, Atteintes aux systémes de traitement automatisé de données, Jurisclasseur pénal,

Art.323-1 à 323-7 , édit.du jurisclasseur, 1997.

[8]لقد صاحب ظهور شبكة الانترنات تطورات كبيرة في شتى المجالات, حيث أصبحت معظم المعاملات التجارية تتم من خلال هذه الشبكة مثل البيع والشراء, مما انجر عنه تطور وسائل الدفع والوفاء وأضحت جزء لا يتجزأ من هذه المعاملات, وفي خضم هذا التداول المالي عبر الانترنت انتهز بعض المجرمون فرصة السطو عليها, حيث ابتكرت عدة طرق من اجل ذلك, على غرار السطو والسرقة, والتحويل الالكتروني غير المشروع للأموال وقرصنة ارقام البطاقات الممغنطة.

[9]لقدأدى التطور التكنولوجي المذهل إلى إحداث ثورة معلوماتية في عالم الاتصالات ونقل المعلومة وكانت المؤسسات البنكية والمصرفية أول من انتفع من تطور الوسائل الالكترونية لتضع على ذمة حرفائها وسائل جديدة للدفع والوفاء لتمكينها من تخطي مخاطر حمل النقود وإجراءات إصدار الأوراق التجارية ولتسهيل الحصول على الخدمات والمشتريات عن بعد.

[10]أ_ **الاحتيال** : يتم ذلك بطرق احتيالية يوهم من أجلها المجني عليه بوجود مشروع كاذب أو يحدث الأمل لديه بحصول ربح ، فيسلم المال للجاني بطريق معلوماتي أو من خلال تصرف الجاني في المال وهو يعلم أن ليس له صفة التصرف فيه ، وقد تتخذ اسم أو صفة كاذبة، تمكنه من الاستيلاء على مال المجني عليه فيتم التحويل الالكتروني للأموال وذلك من خلال اتصال الجاني بالمجني عليه عن طريق الشبكة أو يتعامل الجاني مباشرة مع بيانات الكاذبة التي تساعده في ايهام الحاسب والاحتيال عليه فيسلمه النظام المال.

كما نجد القمار وغسيل الأموال عبر الأنترنت حيث يعد الفضاء السيبراني من أكثر الأسباب التي تشجع على ممارسة القمار عبر الإنترنت مقارنة بممارستها على "الكازينوهات" في الواقع المادي، إذ يمنح الراغب في ممارسة القمار من خلال "الكازينوهات" الافتراضية، الخصوصية وخفاء الشخصية التي يبحث عنها الكثيرون، حيث يستطيع الشخص ممارسة القمار دون حتى أن يغادر غرفة نومه[11].
وكذلك **جريمة السرقة والسطو على أموال البنوك** فتعرف السرقة بأنها اختلاس شيء منقول مملوك للغير بدون رضاه بنية امتلاكه، وتتم سرقة المال المعلوماتي – إن أمكن الوصف- عن طريق اختلاس البيانات والمعلومات، والإفادة منها باستخدام السارق للمعلومات الشخصية- مثل الإسم، العنوان، الأرقام السرية – الخاصة بالمجني عليهم، والإستخدام غير الشرعي لشخصية المجني عليه ليبدأ بها عملية السرقة المتخفية عبر الإنترنت بحيث تؤدي بالغير إلى تقديم الأموال – الإلكترونية أو المادية- إلى الجاني عن طريق التحويل البنكي.

<u>وفي تونس</u> المشرّع التّونسي كان من الأوائل في معالجة المسائل العالقة بالمعلوماتيّة سواء بمناسبة المصادقة على القانون عدد 83 لسنة 2000 المؤرّخ في 9 أوت 2000المتعلّق بالمبادلات والتّجارة الإلكترونيّة أو بمناسبة تنقيح مجلّة الالتزامات والعقود بموجب القانون عدد 57 لسنة 2000 المؤرّخ في 13 جوان 2000 المتعلّق بتنقيح مجلّة الالتزامات والعقود في اتّجاه الاعتراف بالوثيقة الإلكترونيّة والإمضاء الإلكتروني أو بمناسبة تنقيح المجلّة الجزائيّة بموجب القانون عدد89 لسنة 1999المؤرّخ في 2 أوت 1999 في اتّجاه إقرار الجريمة المعلوماتيّة، أو بمناسبة وضع إطار قانوني لضمان السّلامة المعلوماتيّة بموجب القانون عدد 5 لسنة 2004 المؤرّخ في 3فيفري [2004 وضمان حماية المعطيات الشخصيّة بموجب القانون عدد 63 لسنة2004 المؤرّخ في 27 جويلية 2004 [أو

ب_ **الاحتيال باستخدام بطاقات الدفع الإلكتروني**: يعتمد نظام الدفع الالكتروني على عمليات التحويل الإلكتروني من حساب بطاقة العميل بالبنك المصدر للبطاقة إلى رصيد التاجر أو الدائن الذي يوجد به حسابه وذلك من خلال شبكة التسوية الإلكترونية للهيئات الدولية "هيئة الفيزا كارد"، هيئة ماستر كارد" ، وتعطي بطاقة الدفع الإلكتروني الحق للعميل بالحصول على السلع والخدمات على الشبكة عن طريق تصريح كتابي أو تلفوني، بخصم القيمة على حساب بطاقة الدفع الإلكتروني الخاصة به، وتتم العملية بدخول العميل أو الزبون إلى موقع التاجر ويختار السلع المراد شرائها ويتم التعاقد بملأ النموذج الإلكتروني ببيانات بطاقة الائتمان الخاصة بالمشتري، وأمام التطور التكنولوجي أصبحت خلق مفاتيح البطاقات والحسابات البنكية بالطريق غير المشروع ممكنة عبر قنوات شبكة الإنترنت .

[11] وكثيرا ما تتداخل عملية غسل الأموال مع ممارسة القمار عبر شبكة الإنترنت، مما زاد من انتشار أندية القمار الإفتراضية، الأمر الذي جعل مواقع "الكازينوهات" الإفتراضية على الإنترنت محل اشتباه ومراقبة، ومن البديهي أن يأخذ المجرمون بأحدث ما توصلت إليه التقنية لخدمة أنشتطهم الإجرامية ويشمل ذلك طرق غسيل الأموال التي استفادت من عصر التقنية فلجأت الى الإنترنت لتوسعة وتسريع أعمالها في غسيل أموالها غير المشروعة.

ساعدت شبكة الإنترنت القائمون بعمليات غسيل الأموال بتوفير عدة مميزات منها السرعة الشديدة وتخطي الحواجز الحدودية بين الدول وتفادي القوانين التي قد تضعها الدول من أجل إعاقة هذا النشاط ، وكذا تشفير عملياتهم مما يعطيها قدرا كبيرا من السرية، من أجل استثمارها في إقليم أي دولة من العالم، وإعطاء هذه الأموال الصبغة المشروعة.

بمناسبة تنظيم نشاط المتدخّلين في إطار كراس الشّروط الخاص بالخدمات ذات القيمة المضافة من نوع أنترنات أو كرّاس الشّروط الخاص بالخدمات ذات القيمة المضافة التّليماتيكيّة والسمعيّة المصادق عليه بقرار من وزير المواصلات بتاريخ 22 مارس 1997، أو من خلال القانون عدد 61 لسنة2000 المؤرخ في 20 جوان 2000 المتعلّق بتنقيح المجلّة التّجاريّة في اتّجاه الاعتراف بالمقاصة الإلكترونيّة أو قرار وزير الماليّة المؤرّخ في 15 جانفي 2001 في اتّجاه الاعتراف بنظام المبادلات الإلكترونيّة في إطار الإضبارة الوحيدة liasse unique، أو من خلال القانون عدد 51 لسنة 2005 المؤرخ في 27 جوان 2005 المتعلّق بالتحويل الإلكتروني للأموال، أو من خلال القانون عدد 1 لسنة 2001 المتعلق بمجلة الاتصالات أو من خلال قانون عدد 36 لسنة 1994المؤرخ في 24 فيفري 1994المتعلق بالملكية الأدبية والفنية كما هو منقح بموجب القانون عدد 33 لسنة 2009المؤرخ في 23 جوان 2009 في اتجاه حماية البرامج المعلوماتية بواسطة قواعد الملكية الأدبي، إلى جانب جملة من النّصوص القانونيّة الهامّة في اتّجاه تنظيم مجمل النّقاط التّي لها علاقة بتنظيم مهنة مزوّدي الخدمات الرّقميّة واستغلال الشّبكات الرّقميّة وفي الحقيقة أنّ ذلك يأتي في إطار سياسة متكاملة للنّهوض بقطاع تكنولوجيا المعلومات على وجه الإجمال. ويمكن القول إن التشريع غطى أغلب مظاهر الإجرام المعلوماتي سواء كان الاعتداء على الأنظمة المعلوماتية والمعطيات أو شمل المحتوى المعلوماتي[12].

[13]

[12]ويأتي الحديث عن أدوات للتحويل الالكتروني للأموال من خلال القانون عدد 83 لسنة 2000 المؤرخ في 09 أوت 2000 المتعلق بالمبادلات والتجارة الالكترونية ووسائل الدفع الالكتروني بفصله الثاني " بأنها الوسيلة التي تمكن صاحبها بالقيام بعملية الدفع المباشر عن بعد عبر الشبكات العمومية للاتصالات" ، كما أورد القانون عدد 65 لسنة 2001 المؤرخ في 10 جويلية 2001 المتعلق بمؤسسات القرض أن " وضع وسائل الدفع على ذمة الحرفاء وإدارتها تعد من قبيل العمليات المصرفية " وعرف الفصل الخامس وسائل الدفع بأنها " الوسائل بجميع أشكالها التي تمكن من تحويل أموال من شخص إلى شخص آخر مهما كان الأسلوب التقني المستعمل، كما عرف القانون عدد 51 لسنة 2005 المؤرخ في 27 جوان 2005 المتعلق بالتحويل الالكتروني للأموال أداة التحويل الالكتروني بأنها " كل وسيلة تمكن من القيام الكترونيا بصفة كلية أو جزئية بإحدى العمليات التالية:سحب الأموال وإيداعها، تحويل المبالغ المالية، النفاذ للحساب، سحب الأموال وإيداعها ، إعادة شحن وسيلة قابلة للشحن أو تفريغها " وتبدو كلمة التحويل الالكتروني أشمل من عملية الدفع الالكتروني لان الدفع عملية من جملة عمليات التحويل على معنى أحكام القانون 51 لسنة 2005 ويقصد بالدفع الالكتروني استخدام وسائل التكنولوجيا الحديثة كالانترنت وشبكة الهاتف لتسوية الالتزامات ويعرف بأنه عملية تحويل أموال هي في الأساس ثمن لخدمة أو سعلة بطريقة رقمية أي باستخدام أجهزة الكمبيوتر وإرسال البيانات عبر خط هاتفي أو شبكة ما.

[13]**الإطار التشريعي بالنسبة إلى الاعتداء على المحتوى المعلوماتي**

جاء بالفصل الأوّل من الأمر عـ501ـدد لسنة 1997 المؤرخ في 14 مارس1997 والمتعلّق بالخدمات ذات القيمة المضافة أنّ " إنتاج وتقديم وتوزيع وإيواء المعلومات في إطار وضع واستغلال الخدمات ذات القيمة المضافة للاتصالات يخضع لقانون الصحافة وللقانون المتعلّق بالملكية الأدبيّة والفنية." وأضاف الفصل 14 من الأمر عدد501 لسنة 1997 المشار إليه: " يجب أن يكون لكلّ خدمة ذات قيمة مضافة للاتصالات مدير مسؤول عن محتوى الخدمة المقدّمة إلى المستعملين طبقا لأحكام مجلّة الصحافة. ونص الفصل 9 من كرّاس الشّروط الضابط للشروط الخاصة بوضع واستغلال الخدمات ذات القيمة المضافة للاتصالات من نوع أنترنات على ما يلي " تنطبق مقتضيات هذا الفصل على مزودي الخدمات من نوع أنترنات وعلى كلّ الحرفاء المشتركين في الخدمات من نوع أنترنات المالكين لصفحات وموزعي "واب" الذين تمّ إيواؤهم في أنظمتهم. ويجب على مزود الخدمات في إطار تطوير الخدمات من نوع أنترنات في تونس تطوير وإيواء صفحات موزعي "واب" في أنظمته. ويتحمّل المديرالذي يعينه مزود الخدمات طبقا للفصل 14 من الأمر عـ501دد لسنة 1997 المشار إليه أعلاه والذي قدّم اسمه للمتدخّل العمومي المعني المسؤوليّة حول محتوى صفحات وموزعي الواب الذين يقوم بإيوائهم في أنظمته، طبقا لأحكام مجلة الصحافة المشار إليها أعلاه.....ويلتزم المدير بضمان مراقبة دائمة لمحتوى الموزعين المستغلين من قبل مزود الخدمات حتّى لا يقع تمرير معلومات مخالفة للنظام العام والأخلاق الحميدة. ويجب عليهالمحافظة تحت مسؤوليته على نسخة من محتوى الصفحات ومن الموزعين الذين قام بإيوائهم وذلك في شكل وثائق مكتوبة وعلى وسائط مغناطسية مدة سنة بداية من تاريخ توقّف إرسالها لغاية تقديم الحجّة.وفي حالة غلق أو وقف إرسال خدمة ذات قيمة مضافة للاتصالات من نوع أنترنات يلتزم مزود الخدمة حالا بتسليم مجمل الأرشيف، وكل أجهزة قراءة هذه الوسائط إلى المتدخل العمومي المعني". ونصّ كذلك الفصل التّاسع

ولم يكتف المشرع بالإطار التشريعي الموجود بتجريم المحتوى المعلوماتي المخالف، بل جاءت النصوص القانونية الخاصة بتجريم المحتوى المعلوماتي منجمة على مرّ الأيام متى حصلت القناعة بضرورة تأطير الجرائم المستحدثة. فأصبح الاعتداء على الحياة الخاصة والمعطيات الشخصية ولو في فضائها اللامادي جريمة على معنى القانون عدد 63 لسنة 2004 المؤرّخ في 27 جويلية2004، كما أن الاعتداء على الأخلاق الحميدة الواقعة بواسطة المعلوماتية جريمة على معنى الفصل 226 مكرر م.ج بعد تنقيحها سنة 2004 ، وأوردت مجلة الاتصالات الواردة بموجب القانون عدد1 لسنة 2001 عدة جرائم لها علاقة بالاستعمال السيء لأجهزة الاتصالات. وكان المشرع منذ سنة 1994 وضع إطارا خاصا للبرامج المعلوماتية[14].

لكنّ المشرّع التونسي لم ينقح المجلّة الجزائيّة أو النّصوص الخاصّة لجعلها تساير الجرائم المرتكبة بواسطة القنوات الحديثة، ولربما يكون ذلك عائقا أمام تطبيق التشريع الجزائي الخاضع لمبدأ الشرعيّة، الذي من نتائجه الرئيسية التأويل الضيّق للنص الجزائي. وما يعاب على المجلّة الجزائيّة إجمالا أنّها لم تنصّ إلى حدّ الآن، وكقاعدة عامّة، على ارتكاب الجريمة بواسطة الشّبكات المعلوماتيّة، والحال أنّ ذكر الوسيلة هام في بيان العناصر المادية للجريمة، على غرار ما أوردته مجلّة الاتّصالات في مؤاخذة " كل من يتعمد الإساءة إلى الغير أو إزعاج راحتهم عبر الشبكات العموميّة للاتصالات " بوجه عام، أوعلى غرار بعض التّشاريع المقارنة.

وبعد هذا العرض نتناول موضوع الجرائم المالية الالكترونية من زاوية استخدام الإعلامية أوالمعلوماتية كأداة لارتكاب الجرائم لعل أهمها تلك المتعلقة بالبطاقات البنكية **(الجزء الأول)** وباعتبارها موضوعا للاعتداء **(الجزء الثاني)**.

من كرّاس الشّروط الضّابط للشّروط الخاصّة بوضع واستغلال الخدمات ذات القيمة المضافة للاتّصالات التّلماتيكيّة والسّمعيّة على نفس المبادئ، مع التّركيز على ضرورة أن يكون لكلّ خدمة من هذه الأصناف مدير يسأل عند الاقتضاء

[14]ويتلخّص من ذلك أنّ مزود الخدمة، وعادة ما يكون مزود الدخول والإيواء في نفس الوقت، يعتبر مسؤولا على معنى مجلة الصحافة بالنسبة إلى المعلومات التي قام بإيوائها والمخالفة للقانون، وبذلك أعفى المشرّع التّونسي الفقه والقضاء من الاجتهاد في هذه الحدود، ونصّ بصفة صريحة على نفاذ مجلّة الصّحافة على الجرائم المرتكبة بواسطة شبكات ذات خدمة مضافة. وبالتّالي يسأل مدير الخدمة عن جرائم الثّلب والشّتم والتّعريض على ارتكاب الجرائم ضدّ الممتلكات وضدّ أمن الدّولة وضدّ الأشخاص بما في ذلك التّحريض على التّباغض بين الأجناس والأديان والسّكان، كما تقدّم. ويعاب على هذا التّشريع وروده بكرّاس الشّروط المصادق عليه بقرار من وزير المواصلات، وكان من المطلوب أن يرد ذكره بنصوص تشريعيّة، حتّى إن اقتضى الأمر تنقيح المجلّة الجزائيّة أو النّصوص الخاصّة. ولكنّ حسن هذا التشريع أنه كان واضحا في مساءلة مزوّد الخدمة بداية، وإصراره على أن يكون لكلّ خدمة ذات قيمة مضافة مدير يسأل عند الاقتضاء. حيث عوّل المشرّع كثيرا على تدخّل مزوّد الخدمات، وطلب منه أن يراقب مسبّقا محتوى المعلومة، وإذا أخلّت هذه المعلومة بالحدود الجزائيّة، فيسأل بداية المسؤول عن هذه الخدمة، وهو المدير المعيّن والمعلوم من طرف المتدخّل العمومي، وهي قرينة قانونيّة يصعب دحضها. ويتناسق هذا الاتّجاه مع عدّة نصوص أوروبيّة.

ونص كذلك الفصل 9 من كرّاس الشّروط الضابط للشروط الخاصة بوضع واستغلال الخدمات ذات القيمة المضافة للاتصالات من نوع أنترنات على ما يلي: "..... كما يكون الحرفاء المشتركون في الخدمات من نوع أنترنات والمالكون للصفحات وللموزعين الذين تمّ إيواؤهم، مسؤولين عن المخالفات لمقتضيات التشريع الجاري به العمل....."

ويتلخّص من ذلك أنّ التشريع الجاري به العمل يبقى منطبقا على الأفعال التّي يرتكبها المستعمل وخاصة منه المجلّة الجزائيّة والقانون المتعلق بالملكية الأدبيّة والفنية ومجلّة الصّحافة و أحكام الملكيّة الصناعيّة وحماية المستهلك،والقانون المتعلق بالبيع عن بعد، والإشهار التجاري. وجملة الجرائم التّي من الممكن ارتكابها بواسطة شبكات الاتّصالات الحديثة المبيّنة بالقوانين الجزائيّة.

الجزء الأول: المعلوماتية أداة للاعتداء: الجرائم الخاصة بالبطاقات البنكية

اعتمادا على مبدأ تفريد العقاب ونظرية التدرج في تحديد الجزاء المستحق شدد المشرع في تجريم التعامل بالبطاقة البنكية المـــزورة (الفرع الأول) واختار التخفيف في تجريم استعمال البطاقة البنكية الصحيحة بطريقة غير قانونية (الفرع الثاني).

الفرع الأول: تجريم مشدد للتعامل بالبطاقة البنكية المزورة

يعد التزوير في مجال المعالجة الآلية للمعطيات من أخطر طرق الغش وذلك بالنظر إلى الطابع التقني والفني التي تتميز به من جهة والى صعوبة اكتشاف الزور وإثباته من جهة أخرى.

ولئن جرم المشرع التونسي تزوير البطاقة البنكية باعتبارها وسيلة من وسائل الدفع الالكتروني معتبرا هذه الفعلة من قبيل الجنايات التي يعاقب مرتكبها بالسجن والخطية إلا أنه لم يتطرق إلى الأساليب والطرق المتبعة في ذلك (أ).

ولما كانت الغاية الأساسية من تزوير البطاقة البنكية هو الانتفاع بالخدمات التي تؤديها كوسيلة من وسائل الدفع الالكتروني للقيام بالاستيلاءات على أموال الغير، اقر الفصل 17 من قانون 2005 لمستعملها ولمن يقبل الأداء بها نفس العقوبات المقررة لمن قام بالتزوير (ب)[15].

---

[15]ويعتبر في هذا الإطار البطاقات البنكية أحد أهم وسائل الدفع الالكتروني والتي عرفها القانون عدد 51 لسنة 2005 المؤرخ فـــــي 27 جوان 2005 المتعلق بالتحويل الالكتروني للأموال بأنها " كل أداة تحويل الكتروني للأموال تكون وظائفها مغناطيسية أو ذكيـة " .
يقصد بالبطاقة البنكية المغناطيسية تلك البطاقات التي تصدرها البنوك لحرفائها للتعامل بها بدلا من حمل النقود وهي تقوم على مبدأ الدفع المسبق (Pré payement) فهي بمثابة حافظة نقد الكترونية[15].
وقد خلق هذا الانتشار فرصة لمحترفي السرقة والتزوير باستخدام بطاقات بنكية للتحايل والتلاعب خاصة أن هذه النوعية من البطاقات تعتمد في طريقة التعامل بها على النظام المعلوماتي التي تتدفق فيه البيانات والمعلومات والتي تكون فيه النقود عبارة عن بيانات ورموز مشفرة الكترونيا يستطيع محترفو جرائم الحاسب الآلي فكها وتزويرها بهدف الحصول على الأموال بطريقة غير مشروعة.
كما تجدر الإشارة أن سوء استعمال هذه البطاقة تعد فرصة ذهبية لغاسلي الأموال وتجار المخدرات وأقطاب الجرائم المنظمة إذ يمكنهم من ممارسة أنشطتهم والقيام بتحويلات مالية في إطار شرعي تحميه نظم وقواعد الكترونية عمياء.
ومع تزايد معدل الجرائم المصاحبة لاستخدام البطاقات البنكية برزت الحاجة إلى حماية جزائية خاصة يستطاع من خلالها فرض عقوبات على كل فعل يرمي إلى الإضرار بالآخرين سيما أن النصوص الجزائية التقليدية عاجزة عن توفر حماية ناجعة لهذه النوعية من وسائل الوفاء من الاعتداءات التي يمكن أن تقع عليها مما يولد صعوبة في ملاحقة الجاني وتسلط العقوبات الملائمة لخطورة هذه الجرائم[15].
وقد حسم المشرع التونسي الخلاف بصدور القانون عدد 51 لسنة 2005 المؤرخ في 27 جوان 2005 المتعلق بالتحويل الالكتروني للأموال إذ جرم الفصل 17 من هذا القانون تزوير أداة التحويل الالكتروني أو استعمالها أو قبول تحويل باستعمالها بشرط العلم بذلك وأقر لها عقوبة سجنية

أ-طرق وأساليب تزوير البطاقة البنكيـــة

يؤخذ من أحكام المجلة الجزائية أن التزوير أو التدليس يقتضي قانونا القيام بفعل مادي يهدف إلى تغيير الحقيقية في أصل محرر أو كتب موجود من سابق أو بصنع كتب أو عقد أو محرر موضوعه إثبات حق أي أن يستخدم في الإجراءات القانونية على أنه صحيح أو إثبات واقعة منتجة لآثار قانونية بإحدى الطرق المنصوص عليها قانونا أو بأي وسيلة كانت تؤدي إلى إحداث ضرر خاص أو عام ولو كان محتملا.

والملاحظ أن المشرع جرم تزوير البطاقة البنكية دون تحديد الطرق أو الوسائل المتبعة في ذلك، واعتبارا لخصوصية هذا المحور واتخاذها لشكل خاص يميزها عن سائر وسائل الوفاء التقليدية فمن الصعب أن يكون تزويرها بإحداث تغيير على البيانات الموجودة على صدر البطاقة أو ظهرها وبذلك فان المقصود بالتزوير هنا هو الاصطناع.

والاصطناع هو طريقة من طرق التزوير المادي ويعني خلق محرر بأكمله ونسبته إلى غير محرره وهو إنشاء محرر بكامل أجزائه على غرار أصل موجود أو خلق محرر على غير مثال سابق.

والواقع أن تزوير البطاقة البنكية أمر صعب لكنه ليس مستحيلا ويتخذ عادة عدة أشكال يمكن تقسيمها إلى طريقتين: الطريقة الأولى تتمثل في تزوير كلي للبطاقة والثانية تتمثل في تزوير جزئي للبطاقة.

1-طرق وأساليب التزوير الكلـــي

تتم عملية التزوير الكلي للبطاقة البنكية باصطناع البطاقة كاملة ثم يقع تقليد الرسوم الخاصة على جسم البطاقة وتغليفها وإلصاق الشريط المغناطيسي أو الشريحة الالكترونية كل حسب موضعه على صدر البطاقة أو ظهرها، ثم القيام بالطباعة وتشغيلها بتغذيتها بالمعلومات التي حصل عليها المزور من البطاقة الصحيحة.

ومما لا شك فيه فان إنتاج بطاقة بنكية مزورة يستدعي ضرورة توفير جملة من التجهيزات والمواد الأولية اللازمة لصناعة الشريط المغناطيسي أو الشريحة

تصل إلى 10 سنوات والخطية بعشرة آلاف دينار ، كما جرم بالفصل 18 منه كل استعمال لوسيلة تحويل الكتروني دون إذن صاحبها ورتب عن ذلك عقوبة السجن بثلاث سنوات والخطية بثلاثة آلاف دينار.
إن أساس البحث عن حماية جزائية للبطاقة البنكية يكمن في القيمة التسويغية والاقتصادية التي تتمتع بها باعتبارها وسيلة حديثة من وسائل الوفاء تزايد التعامل بها في ميدان التجارة الالكترونية.

إضافة إلى آلات وأدوات تصوير ضوئي Scanner وآلات طباعة الشبكة الحريرية وما يلائمها من حبر خاص وآلة طباعة الحروف النافرة وآلة تشفير خاص للبيانات التي يتم تخزينها على الشريط المغناطيسي أو على الشريحة الالكترونية وآلة لتغليف جسم البطاقة كل ذلك بعد الحصول على معلومات تتعلق بأسماء وأرقام أصحاب البطاقات الصحيحة والمتداولة بواسطة أشخاص مجندين لذلك ، وبإتمام عملية الصنع تخرج نسخة ثانية من بطاقة صحيحة ومتعامل بها ليتم استعمالها في الاستيلاءات[16].

أما الطريقة الثانية للتزوير الكلي فتتم حين يتوفر الرقم السري الخاص بالبطاقة الحقيقية فيقوم المزور باستعمال بطاقة بلاستيكية بنفس الحجم المعتاد خالية من أية بيانات ويثبت عليها الشريط المغناطيسي ثم يقوم بتشفير الرقم السري ونسخه بواسطة جهاز خاص ليصنع بذلك أي عدد ممكن من البطاقات لاستخدامها في سحب الأموال من أجهزة الصرف الآلي التي تقبل رؤوسها القارئة المعلومات المدونة على الشريط المغناطيسي فقط وبغض النظر عن وجود البلاستيك الذي يشكل البنيان المادي لجسم البطاقة أو باقي البيانات المثبتة كاسم الحامل أو رقم الحساب البنكي وهذه الطريقة هي من اخطر طرق التزوير ويطلق عليها اسم التحايل بالبطاقة الفارغة .

2-طرق **وأساليب التزوير الجزئـــي**

يستفيد المزور في هذه الحالة من جسم البطاقة الحقيقية وما عليها من رسوم خاصة وحروف بارزة ليقوم بتزوير البطاقة عن طريق صهر ما عليها من أرقام بارزة لبطاقة حقيقية انتهت فترة صلاحيتها أو إعادة قولبة رقم الحساب الذي تعمل عليه البطاقة بأرقام حساب آخر أو تقليد الشريط المغناطيسي عن طريق محو ما عليه من بيانات وإعادة تشفيره بمعلومات جديدة صحيحة مسروقة وقد يتم إجراء العمليتين معا.

كما يمكن أن يقوم المزور في هذه الحالة بكشط شريط التوقيع الموجود على ظهر البطاقة بشريط آخر يتضمن توقيعه أو بمحوه آليا أو كيميائيا ووضع شريط آخر.

ولعل الإشكال الذي يطرح هنا يتعلق بمدى إمكانية تطبيق الأحكام العامة لجريمة التزوير على الشريط المغناطيسي أو الشريحة الذكية المحضورة بجسم

[16]قد جرم الفصل 11 من قانون 91-1382 الصادر في 1991/12/30 الفرنسي صناعة أو بيع أو عرض لبيع أو حيازة أدوات أو آلات أو خامات مما يستعمل في تصنيع البطاقات بغير سبب شرعي.

البطاقة إذ قد يتراءى للبعض بأن هذه الأخيرة تنتفي عنها صفة ومقومات المحرر سواء كان رسميا أو عرفيا على اعتبار أن البيانات المخزنة في هذا الشريط لا يمكن رؤيتها بالعين المجردة أو بطريق اللمس ولا يمكن الاطلاع عليها إلا بوسائل خاصة ، إلا أن هذا الرأي قد وقع تجاوزه على اعتبار أنه لم يعد يتناسب مع الأساليب الحديثة التي يستخدمها الجناة نتيجة تطور الحذق الإجرامي وهو ما دفع المشرع إلى توسيع مجال انطباق الفصل 172 من المجلة الجزائية بموجب القانون عدد 89 لسنة 1999 المؤرخ في 1999/08/02 وذلك بأن أصبح يشمل أي سند سواء كان ماديا أو غير مادي من وثيقة معلوماتية أو الكترونية وميكروفيلم وميكروفيش وذلك تماشيا مع التطور في ميدان الاتصالات الذي أفضى إلى نوع جديد من التعامل التجاري عن طريق هذه الوسائل[17].

ولا بد من التذكير أن جريمة تزوير البطاقة البنكية تستوجب لقيامها توفر القصد الجنائي العام المتمثل في علم الجاني بأنه يقوم بتغيير الحقيقة في إحدى المحررات المصرفية ويترتب عن ذلك ضررا حالا أو احتماليا بأحد الأشخاص وبالتالي ينتفي القصد العام ولا تقوم الجريمة في جانب موظف البنك الذي يثبت أن البيانات المدلى له بها هي بيانات كاذبة ولم يكن عالما بذلك.

أما بالنسبة للقصد الجنائي الخاص فيتمثل في نية الجاني في استعمال البطاقة المزورة استعمالا غير مشرع في الغرض أو الأغراض التي أعدت من أجلها بمعنى أن أراده الجاني تصرف إلى تغيير الحقيقة في البطاقة لاستخدامها فيما زرت من أجله حتى لو لم يستخدمها فعلا أو أن يعدل عن استعمالها.

ب-استعمال البطاقة البنكية المزورة وقبول الأداء بواسطتها

نص الفصل 17 من قانون 2005 على معاقبة كل من يستعمل بطاقة بنكية مزورة أو يقبل الأداء بواسطتها وهو عالم بذلك بنفس العقوبات المقررة للمزور.

وتجدر الإشارة أن نظام العمل بالبطاقة البنكية يشبه النظم القانونية التي تحكم حوالة الحق أو تلك التي تحكم الوكالة إلا أنه لا يدخل ضمن هذه الأنظمة لان لهذه البطاقة طبيعة قانونية خاصة فهي تختلف عن النقود الورقية أو المعدنية المتداولة لأنها تفتقد إلى خاصية التداول التي تتصف بها النقود فضلا عن أنها وسيلة لدفع

[17]وتجدر الإشارة أن الحصول على المعلومات الخاصة بالبطاقة الأصلية للقيام بعملية التزوير يكون بانتهاج طرق متعددة لعل أهمها:
*التواطؤ مع العاملين في الجهة المصدرة أو المختصين في تغذيتها بالمعلومات أو مع العاملين بالمحلات التجارية.
*اختراق البيانات والدخول غير المشروع إلى شبكات الكمبيوتر في البنوك والحصول من خلالها على أدق التفاصيل المتعلقة بحامل البطاقة.
*وضع جهاز قارئ الكتروني في فتحة إدخال البطاقة في أجهزة الصرف الآلي ومن ثم تسجيل البيانات الخاصة أو وضع كاميرا صغيرة الحجم في مكان فوق فتحة جهاز الصرف الآلي وتصوير عملية إدخال الرقم السري ليقع بعد ذلك إنتاج بطاقة مستنسخة من البطاقة الأصلية.

النقود لذلك فلا تنطبق عليها النصوص الجزائية المتعلقة بتزييف العملة كما أنها ليست شيكا لان الشيك واجب السداد بمجرد الاطلاع عليها فضلا عما تتميز به المعاملات بالبطاقة البنكية من بعد بين أطراف التعامل وذلك باستخدام التكنولوجيات الحديثة للاتصال كالانترنات وشبكة الهاتف.

وقد تعرض الفصل الأول من قانون 27 جوان 2005 إلى العمليات التي يمكن القيام بها بوساطة البطاقة البنكية باعتبارها أداة للتحويل الالكتروني للأموال وهي تحويل المبالغ المالية وسحب الأموال وإيداعها والنفاذ إلى الحساب وإعادة شحن وسيلة قابلة للشحن أو تفريغها. وبالتالي فان القيام بإحدى العمليات المذكورة باستعمال بطاقة بنكية مزورة يعد عملا مجرما على معنى أحكام الفقرة الثانية من الفصل 17 من القانون المذكور.

ولا بد من الملاحظة أن تزوير البطاقة البنكية لا يعد أن يكون إلا عملا تحضيريا لان الغرض المنطقي لعملية التزوير هو الاستعمال للتحيل على الغير والاعتداء على أمواله. ولأجل ذلك اعتبر المشرع هذه العملية جريمة في حد ذاتها ووصف عليها عقابا صارما ومستقلا عن عقاب التزوير خلافا لما جاء صلب الفصل 411 مكرر من المجلة التجارية حين جرم تزييف الشيك أو تزويره دون أن يتعرض إلى استعمال الشيك المزور، والحال أن الجريمتين منفصلتين وهو ما يتأكد بالرجوع إلى القراءة العامة لجريمة التدليس التي جاءت بها أحكام المجلة الجزائية إذ نص الفصل 177 منها على جريمة استعمال المحررات كما نصت الفصول 193 إلى 199 على جريمة استعمال الأوراق المفتعلة وبالتالي فان جريمة التزوير منفصلة عن جريمة استعمال المزور ، فكل منهما جريمة مستقلة بذاتها إذ من الممكن أن يكون من قام بالتزوير شخصا ما ومن يقوم باستخدام المزور شخص آخر ويترتب عن ذلك عدة نتائج قانونية وهي:

*إمكانية معاقبة مستعمل البطاقة المزورة مع العلم بذلك دون أن يكون فاعلا أصليا أو مشاركا في جريمة التزوير.
*إمكانية مساءلة من استعمل البطاقة المزورة حتى وان كان من زورها شخص مجهول أو غير مسؤول جزائيا لصغر سنه أو لجنونه أو لغير ذلك من الأسباب.
*سقوط الدعوى عن فعل التزوير بمرور الزمن لا يمنع من مساءلة المستعمل عن فعل الاستعمال ما لم يكن هذا الفعل قد سقطت دعواه بمرور الزمن.
وما تجدر الإشارة إليه أنه ولتوفر جريمة الاستعمال يجب أن يكون المستعمل على بينة من أن البطاقة مزورة ويقوم مع ذلك باستخدامها فيما أعدت له وإبرازها على

أنها صحيحة، أما مجرد إظهارها للغير أو تقديمها له لمجرد التباهي أو إشباع الرغبة في الظهور بمظهر لائق فلا يشكل جريمة الاستعمال.

ونظرا لخطورة تزوير البطاقة البنكية والأضرار التي تنجم عنه سواء على المنتفع بالبطاقة أو على المؤسسة المصرفية المصدرة لها فقد جرمت الفقرة الثالثة من الفصل 17 لقانون 2005/06/27 قبول التحويل بالبطاقة البنكية المزورة مع العلم بذلك.

ولئن جاءت عبارة هذه الفقرة عامة في تجريم قبول كل عمليات التحويل فان استخدام البطاقة البنكية المزورة يكون عادة في عملية الوفاء سواء كان بشكل مباشر أو بشكل غير مباشر عبر شبكة الانترنات ، هذه الطريقة الأخيرة تلجأ إليها عادة العصابات المنظمة للاستيلاء على الأموال على اعتبار أن استخدام البطاقة البنكية المزورة يعد فرصة ذهبية لغاسلي الأموال وأقطاب تجارة المخدرات والجرائم المنظمة إذ أنها تمكنهم من ممارسة أنشطتهم وتحويلاتهم المالية في إطار شرعي، والغالب أن تكون هذه الممارسة مشتتة بين عدة بلدان ، إذ يتم عادة تجميع المعلومات اللازمة عن البطاقة البنكية الصحيحة في دولة ويتم إعداد البطاقة المزورة في دولة أخرى ويجري ترويجها واستخدامها في دولة ثالثة ويكون التحويل لدولة رابعة [18].

ونظرا للطبيعة اللامادية لهذه الجرائم والخصوصية التي تتميز بها فإنها تثير صعوبات عملية عديدة بالنسبة للسلط المكلفة بالبحث والاستدلال، ولا يمكن تذليل هذه الصعوبات على مستوى الإثبات إلا بتوفر حد أدنى من معرفة الجوانب الفنية للمعلوماتية إذ أن هذه الجرائم تتسم بصبغة فنية دقيقة بوصفها ترتكب باستعمال تكنولوجيا عالية وفي فضاء الكتروني لا تدركه الحواس مما يحصل من عملية استخلاص الأدلة في شأنها أمرا عسيرا.

---

[18] وفي الواقع فان عملية استخدام البطاقة البنكية للدفع الالكتروني عبر شبكة الانترنات تمر بثلاث مراحل:

المرحلة الأولى: مرحلة البيع: بعد ملء النماذج والضغط على خانة التأكيد (Submit) من قبل صاحب البطاقة يقع إرسال نموذجا آخر لتحديد السلفة المطلوبة وتسجيل رقم البطاقة ونوعها وصلاحيتها وبالضغط مرة أخرى على خانة التأكيد (Valider) ينتقل النموذج الكترونيا إلى البريد الالكتروني للتجار في اللحظة ذاتها.

المرحلة الثانية: مرحلة الاستئذان بالدفع: يتم إرسال النموذج الكترونيا إلى بنك التاجر ومن ثم تحويله إلى بنك صاحب البطاقة الذي يسمي البنك المصدر من خلال أحد الشبكات وبوصول إلى البنك المصدر يتم تحديد ما إذا كان الرصيد البنكي كافيا من عدم ذلك، وفي صورة الإيجاب تبتدئ المرحلة الثالثة.

المرحلة الثالثة: مرحلة الإبراء: يعود النموذج من خلال الخط الالكتروني نفسه إلى صاحب البطاقة (مستعملها) يصاحبها إشارة مفادها أن عملية الدفع قد أنجزت حيث يحصل التحويل الحالي الكترونيا من حساب صاحب البطاقة لدى البنك المصدر إلى حساب التاجر في بنكه وهكذا تنتهي عملية الدفع بالبطاقة عبر الانترنات وهي عملية لا تستغرق سوى بعض الثواني. ونتيجة للسرعة التي تتم بها عملية تحويل الأموال الكترونيا فان التعرف على الجاني سواء كان مستعمل البطاقة البنكية المزورة أي الذي قام بالتحويل أو من قبل الأداء بها بواسطتها وهو يعلم أنها مزورة أمرا صعبا ، ويعود ذلك بالأساس إلى سهولة إعدام وإتلاف المعطيات الالكترونية في أوقات قياسية والقدرة على فسخها أو تغيير محتواها ومن ثمة طمس عناصر الإثبات والتي تكون عادة مشتتة بين عدد غير محدود من الدول.

ومن هذا المنطلق فان الأشخاص المباشرين للأبحاث في هذه الجرائم يجب أن يكونوا على دراية بتقنيات وأساليب التحقيق في الجرائم المعلوماتية ومكتسبين للمؤهلات الكفيلة بالتوصل إلى استخلاص عناصر الإثبات الملائمة لمواجهة هذه الظاهرة الإجرامية والحد من انتشارها الناتج عن توسع دائرة استخدامات الحسابات الآلية وشبكة المعلومـات الدولية.

ولكل ذلك نص الفصل 19 من قانون 27 جوان 2005 على أن معاينة المخالفات لأحكام هذا القانون تقع "من قل أعوان الضابطة العدلية والأعوان المحلفين التابعين للوزارة الحالية والأعوان المحلفين التابعين للوزارة المكلفة بتكنولوجيا الاتصال وللوكالة الوطنية للمصادقة الالكترونية ".

وبذلك وعلى عكس الجرائم التقليدية فان النيابة العمومية أصبحت تجد مزاحمة على مستوى إثارة الدعوى العمومية أو معاينة الجرائم من قبل الإدارة وهياكلها المختصة وذلك بالنظر إلى الطابع الفني والتقني لهذا النوع من الأفعال.

الفرع الثاني: تجريم مخفف لاستعمال البطاقة البنكية الصحيحة بطريقة غير قانونية

ينص الفصل 18 من قانون 27 جوان 2005 المتعلق بالتحويل الالكتروني للأموال على أنه " يعاقب بالسجن مدة ثلاث سنوات وبخطية قدرها ثلاثة آلاف دينار كل من استعمل أداة تحويل الكتروني للأموال دون إذن صاحبها" .

لقد تضمن هذا الفصل على عقوبة مخففة مقارنة بالعقوبة المنصوص عليها بالفصل 17 المتعلق بجرائم التزوير ومرد ذلك أن استعمال البطاقة البنكية في هذه الحالة هو استعمال لبطاقة صادرة عن الجهة المختصة بإصدارها إلا أنها استعملت من قبل غير من صدرت باسمه.

وإجمالا فان هذا الاستعمال يكون إما باستخدام جسم البطاقة مع رقمها السري (أ) أو باستخدام الرقم السري للبطاقة فقط (ب).

أ-الاستعمال غير القانوني للبطاقة الصحيحة من طرف حائزها

يستطيع الحائز للبطاقة البنكية المسروقة أو الضائعة استعمالها إما في الوفاء بثمن السلع أو الخدمات أو في سحب الأموال من أجهزة الصرف الآلي، ولقد اعتبرت تعاملات آلة الصراف الآلي أو الوفاء مباشرة لدى التجار دوما على أنها آمنة جدا لأنها تتطلب إدخال الرقم السري في جهاز الصراف الآلي أو في الجهاز المستعمل في المحلات التجارية لذلك فان عمليات الاحتيال من خلالها تكون نادرة

ولكنها عندما تحدث فإنها توفر طريقة لحصول الجناة على مبالغ مالية كبرى مما يؤدي إلى زعزعة ثقة الحريف بأمن شبكة أجهزة الصراف الآلي وشبكة الدفع المباشر.

وتتعدد طرق الحصول على المعلومات الخاصة بالبطاقة البنكية وخاصة رقمها السري لغاية استعمالها وتتمثل خاصة فيما يلي:

- **كتابة الرقم السري على البطاقة**

يعمد البعض إلى كتابة تفاصيل أرقام التعريف الشخصية الخاصة بهم على البطاقة نفسها أو على مستندات يكون الرقم فيها واضحا للشخص الذي يسرق البطاقة أو الذي يجدها بعد ضياعها فلا يجد صعوبة في استعمالها.

- **إعطاء الرقم السري للغير**

غالبا ما يفصح حاملو البطاقات عن أرقامهم السرية لبعض الأشخاص المقربين منهم مما يجعل من سرية هذه الأرقام أمرا عقيما.

ومن السرقات التي تمت بهذه الطريقة في فرنسا سنة 1994 قيام أحد الأشخاص أثناء تناول الغداء مع صديقته وبحجة اختبار ذاكرتها طلب معرفة الرسم السري لبطاقتها البنكية وعندما أخبرته به قام بسرقة بطاقتها وسحب أموالها من جهاز الصراف الآلي. وفي هذه الحالة يعد استعمال البطاقة من قبل الغير استعمالا غير مشروع.

أما في تونس فقد تمكن أحد الأشخاص العاملين بمركز نداء من ربط علاقة مع امرأة فرنسية ثرية وأوهما أنه فرنسي فوعدته بتمكينه من هدية بمناسبة رأس السنة الميلادية وللغرض مكنته من بيانات بطاقتها البنكية فاسحة له المجال لاقتناء ما يريد من الهدايا وقد قام باستعمالها في ست عمليات شراء هواتف جوالة من شركة اتصالات إلا أن المرأة الفرنسية تفطنت إلى أن العمليات البنكية التي ظهرت لها كانت بالدينار التونسي وأن مخاطبها لم يكن متواجدا في فرنسا ولم يكن فرنسيا رغم أن مركز النداء كان يستعمل أرقاما توحي أن الشخص متواجد في فرنسا ، لذلك اعترضت صاحبة البطاقة على المعاملات، وقد تمت إحالة ذلك الشخص على المجلس الجناحي من أجل خيانة الأمانة الموصوفة واستعمال أداة تحويل الكتروني دون إذن صاحبها طبق الفصل 297 م ج والفصل 18 من القانون عدد 5 المؤرخ فـــي 27 جوان 2005 المتعلق بالتحويل الالكتروني للأموال.

والملاحظ أنه عند قيام الغير بسرقة البطاقة أو يعثر عليها بعد ضياعها، فانه يتجه عادة الى استخدامها فورا مستغلا بذلك الفترة التي تقع بين تاريخ الضياع أو

السرقة وتاريخ تقديم الاعتراض الى الجهة المصدرة طبقا للإجراءات المنصوص عليهـــا بالفصل 10 مـــن قانون 27 ماي 2005[19].

ب- الاستعمال غير القانوني للبطاقة باستخدام الرقم السري

لا شك أن الاستخدام غير المشروع لبطاقة الدفع الالكتروني يمثل خطرا يهدد السوق التجارية، خاصة ما تعلق منها بالسداد أو مقابل الوفاء ويحصل المستهلك أو المشتري غير راغب في هذه المعاملة محبذا العودة إلى أسلوب الوفاء التقليدي بالنقود أو الشيك.

لذلك يظهر خطر الاستخدام غير المشروع للبطاقة البنكية جسيما على التجارة الالكترونية متى تم التلاعب بهذه البطاقة عن طريق شبكة الانترنات ومواطن الخطورة أن التجارة الالكترونية تعتمد على نظام معلوماتي متكامل من حيث الإشهار والتسويق والمفاوضات وإبرام العقد وتنفيذه والحصول على المقابل المالي، والمعلوم أن نظام الدفع الالكتروني مبني على أساس عمليات التحويل الالكتروني من حساب صاحب البطاقة بالبنك المصدر إلى رصيد التاجر بالبنك الذي يوجد به حسابه من خلال شبكة تسوية الكترونية للهيئات الدولية (الفيزا كارت والماستر كارت)، حيث تعطى البطاقة البنكية للحريف الحق في الحصول على السلع والخدمات عن طريق الانترنات.

وقد تحولت معظم البطاقات البنكية العالمية المعروفة أمثال فيزا وماستركارت إلى وسيلة دفع الكترونية فعلية عن بعد يمنح حاملها رقما سريا يستخدمه في عملية الدفع أو التحويل أو سحب الأموال، لكن يتبع ذلك مخاطر متعلقة بالقرصنة المعلوماتية المحتملة للأرقام السرية التي تتجول داخل شبكة الانترنات.

فقد تمكن بعض الهواة والمحترفين من معتادي التعامل مع شبكة الانترنات الذين يطلق عليهم تسمية هاكر Hackers من التقاط أرقام البطاقات البنكية الخاصة من الشبكة واستخدموا أرقامها في الحصول على السلع وخصم ثمنها من حسب الحامل الشرعي لهذه البطاقة وهناك عدة طرق يتبعها القراصنة للحصول

[19]ويفضل الحائز للبطاقة المسروقة أو المفقودة التعامل مع التجار الذين يستخدمون الأجهزة اليدوية لان الحماية للبطاقة في هذه الحالة تكون أقل بكثير من الحماية الممنوحة للبطاقة من خلال الأجهزة الالكترونية.
وفي الواقع فان البطاقات البنكية المغناطيسية قد تناقص استعمالها حاليا مقابل انتشار البطاقات ذات الشريحة البنكية والتي تستوجب إدخال الرقم السري للتعامل بها مع التاجر إلا أن البطاقات ذات الشريط المغناطيسي لازالت منتشرة في الولايات المتحدة الأمريكية .
فعندما يقوم الحائز للبطاقة بتقديمها إلى التاجر وفاء للمشتريات أو الخدمات التي حصل عليها، فانه يقوم بتوقيع الفاتورة إما مقلدا لتوقيع صاحبها أو أن يمحو توقيع الحامل على البطاقة ويضع توقيعه بدلا منه لتطابق توقيعه على الفاتورة مع التوقيع على البطاقة ، وفي هذه الحالة فان الجاني يعد مرتكبا لجريمة السرقة وتزوير البطاقة البنكية.
وفي الواقع فان البطاقة ذات الخط المغناطيسي (الخط الأسود الموجود من خلف) والتي يمكن قراءتها بالجهاز اليدوي أصبحت قليلة الاستخدام حيث تناقص استخدامها تدريجيا إلا أنها لا تزال منتشرة في الولايات المتحدة الأمريكية ، أما في بقية دول العالم، فانه يتم حاليا استخدام الجهاز الذي يحتاج للرق السري والذي يعد أكثر أمانا.

على بيانات البطاقة البنكية واستعمالها بطرق غير مشروعة للحصول على المبلغ والخدمات وهذه الطرق هي:

1-اختراق منظومة خطوط الاتصالات

وهي الخطوط التي تربط الحاسب الآلي للمشتري بذلك الخاص بالتاجر ويعد الجاني هنا بمثابة من يتنصت على مكالمة هاتفية وهذا الأسلوب من أخطر ما يهدد التجارة عبر الشبكة، ذلك أن الدافع الأساسي وراء اللجوء إليه يتمثل في رغبة كامنة في نفوس محترفي إجرام التقنية في التفوق على نظم الحماية وتعقيداتها[20].

وإمعانا في التحدي يقوم معظم العصابات التي تضم قراصنة البطاقات بنشر هذه المعادلات وبيان الكيفية التي يمكن من خلالها إتباعها خطوة بخطوة للحصول على الأرقام الخاصة بالبطاقات غبر مواقعهم على شبكة الانترنات.

ورغم صعوبة تحديد شخصية محترفي قرصنة أنظمة المعلومات إلا أنه يمكن تحديد كيفية الاختراق وزمانه وكلمة السر التي استخدمت في الاختراق وذلك من خلال مراجعة ملفات الدخول للنظام والملفات التأمينية الخاصة بها على نحو يسمح بجمع أكبر قدر من الأدلة التي قد تساعد على معرفة الجاني.

2-تقنية تفجير المرتع المستهدف

يعتمد هذا الأسلوب على ضخ مئات الآلاف من الرسائل الالكترونية من جهاز الحاسب الآلي للمتعدي (القرصان) إلى الجهاز المستهدف بهدف التأثير على ما يعرف بالسعة التخزينية بحيث يشكل هذا الكم الهائل من الرسائل الالكترونية ضغطا يؤدي إلى تفجير الموقع العامل على الشبكة وتشتت المعلومات والبيانات المخزنة فيه لتنتقل بعد ذلك إلى الجهاز الخاص بالقرصان ليتسنى له الحصول على كل ما يحتاجه من أرقام وبيانات خاصة بالبطاقات البنكية .

يجرم الفصل 199 من المجلة الجزائية هذا النوع من الأفعال إذ يعاقب الفقرة الرابعة منه بالسجن بخمس سنوات من أدخل بصفة غير شرعية بيانات بنظام معالجة معلوماتية من شأنها إفساد البيانات التي يحتوي عليها البرنامج أو طريقة تحليلها أو تحويلها والمقصود بذلك إدخال معلومات ببرنامج معلوماتي تكون سببا في إفساد ما هو مخزن به من معلومات وهو ما يعبر عنه باللغة الفرنسية بالفيروس (Virus) الذي يتسبب في إفساد أو تعطيل هذا البرنامج ، أو في الاستحواذ عليه

[20] برهان عزيزي، **"التنصت الهاتفي : أذن تشتكي وجريمة تستنطق"، الإخبارية،2017.**

أو إفساد طريقة سيره وتصبح العقوبة مضاعفة إذا وقع اقتران الفعل المذكور من طرف شخص بمناسبة نشاطه المهني.

3-أسلوب الخداع

تمثل المواقع الالكترونية المزورة طريقة مهمة وشائعة للاحتيال وسرقة الأموال عبر الانترنات وهي مشكلة يمكن أن يواجهها أكثر أناس حرصا خلال التسوق على الانترنات والسبب في ذلك أن الجناة الذين يتبنون هذه الوسيلة يتمتعون بدرجة عالية من الاحتراف والخبرة.

ويقوم أسلوب الخداع على إنشاء موقع الكتروني وهمي يحمل اسما معروفا لمؤسسة تجارية أصلية موجودة على الشبكة ويكون بالشكل نفسه وحتى اسم النطاق يكون قريبا جدا من اسم النطاق الحقيقي فيتم إرسال الرابط للضحية بطريقة أو بأخرى وغالبا ما يكون عبر الرسائل الالكترونية الذي يقوم بتعبئة بياناته والتي لا تذهب إلى المكان الصحيح وإنما إلى أيدي المختالين.

وعلى اعتبار أن المواقع الالكترونية هي في الأصل نتاج فكري للإنسان فان من حق صاحبها أن يدعي ملكيته وأن يسعى لحماية تلك الملكية ، لذلك فان إنشاء موقع وهمي يعد اعتداء على حق الملكية الأدبية والفنية المجرم بالفصل 51 من القانون عدد 36 لسنة 1994 المؤرخ في 1994/02/24 المتعلق بالملكية الأدبية والفنية[21].

[21]وفي الواقع فان استعمال بطاقة بنكية صحيحة بدون موافقة صاحبها يرتبط عادة بارتكاب عدة جرائم أخرى وذلك بالنظر إلى الطريقة التي يقع الحصول بها على البطاقة البنكية أو على الرقم السري الخاص بها وعلى ارتباط الجاني عادة بأطراف أجنبية وعصابات دولية مختصة من ذلك ما توصلت إليه إحدى الفرق الأمنية المختصة بالجرائم الحالية في تونس سنة 2010 حين تمكنوا من الكشف على أحد الأشخاص كان قد تسوغ محلا بجهة الحمامات وجهزه بشبكة انترنات ذات تدفع عالي وتمكن من خلال استعمال منظومة " ميرك Mirc " الانخراط في شبكة دولية لعناصر من أكثر من عشرين دولة أحدثت سوقا لبيع " شيفرات" البطاقات البنكية الدولية . وقد تمكن المتهم من الحصول على هويات رقمية وأرقام بطاقات بنكية مسروقة من مواقع تجارية الكترونية وكان يتحصل على تلك المعطيات مقابل مبالغ مالية بالدولار الأمريكي في حسابات افتراضية تسمى " واب ماني Web Money " ثم أصبح يبيع الهويات بتلقي أموال في حسابه الافتراضي أو عبر حوالات بريدية دولية يتم تسلمها من مكاتب البريد الموجودة بتونس ، وبالاشتباه في اسمه أصبح ينتدب شخصين غير معروفين من قبل الشركة الأمريكية (وسترن يونيون) للقيام بعملية السحب وقد أثبتت الأبحاث أن المتهم على علاقة بمجموعة من الهاركز من جنسيات مختلفة كانوا يتاجرون في أرقام البطاقات البنكية ويتم تبادل الهويات الرقمية المسروقة مثل عناوين البريد الالكتروني واسم المستخدم وكلمة المرور وأرقام البطاقات وذلك عبر عمليات الاصطياد أو ما يعرف " بالفيشينغ Phising " ثم يقع استعمال برنامج للإرسال الجماعي ويقع إنشاء صورا لمواقع مختصة في البيع يقومون ببيعها لأصحاب تلك العناوين البريدية فيقوم العديد منهم بتصميم البيانات بإشعارات وهمية بروابط تلك المواقع المزيفة التي هي صور لمواقع أصلية مثل مواقع بنوك أو مغازات، كما تبين أن بعض الهاكرز يستعملون أفلاما إباحية لاصطياد الضحايا وذلك بالإعلان عن بيع أفلام جنسية من كافة أنحاء العالم ولمن يرغب في الشراء فما عليه إلا تعمير استمارة افتراضية ببياناته الشخصية ومن هنا تتم عملية الاصطياد وقد أحالت النيابة العمومية بتونس في هذه القضية المتهمين من أجل السرقة والتحيل واستعمال أداة تحويل الكتروني دون إذن صاحبها وتكوين عصابة ووفاق للانخراط في عصابة ووفاق والمشاركة فيه بصد ارتكاب اعتداء على الأملاك والمشاركة في ذلك والنفاذ بصفة غير شرعية بجزء من نظام البرمجيات والبيانات المعلوماتية والتعامل بين مقيم وغير مقيم دون ترخيص من البنك المركزي طبق الفصول 28 و 43 و44 من الأمر عدد 608/77 المؤرخ في 27 جويلية 1977 والفصول 32و35و36و37 من القانون عدد 18/76 المؤرخ في 1976/01/21 والفصول 32و258 و264 و291 و131 و132 و199 مكرر من المجلة الجزائية والفصل 18 من القانون عدد 51 لسنة 2005 المؤرخ في 27 جوان 2005 المتعلق بالتحويل الالكتروني للأموال.

الجزء الثاني: المعلوماتية موضوع للاعتداء: الجرائم الخاصة بالبرامج(الأنظمة)

لا بد من تحديد موضوع الجريمة المعلوماتية وهو البرنامج في النظام المعلوماتي (فرع أول) للانتهاء لاحقا إلى ضبط عناصر التجريم (فرع ثان).

الفرع الأول: موضوع التجريم: البرنامج المعلوماتي

يعرف البرنامج بكونه " مجموعة من الإيعازات والأوامر المتسلسلة المقدمة الى الآلة الحاسبة بلغة وصيغة تدور حول المكونات غير المادية للجهاز. ينقسم البرنامج كما هو معلوم الى نوعين : برنامج الإستغلال ويشمل كل البرامج التي تسير عمل الآلة في حد ذاتها أو تلك التي تسير الخدمات والصيانة. وبرامج التطبيق التي " تشمل البرامج التي تهدف الى مساعدة المستعمل على مجابهة مشاكل خاصة به وحلها بواسطة الحاسوب"[22].

وقد تعرض الفصل 199 جديد من م.ج. الى صورة الإعتداء على البرنامج في فقرته الثالثة: "يعاقب بالسجن مدة ثلاثة أعوام وبخطية قدرها ثلاثة ألاف دينار كل من يعتمد إفساد أو تدمير نظام معالجة معلوماتية".

الإفساد و التدمير يمكن أن يتخذ صورا عديدة إذ قد يعمد الجاني الى حجز رمز النفاذ الى نظام المعالجة المعلوماتية وهو ما يعني عدم إمكانية إستعمال النظام برمته أو إلى تنفيذ برنامج يعيق سير نظام المعالجة سواء بصفة دائمة بإدخال فيروس أو بصورة دورية عن طريق القنابل المنطقية.

وتتعدد أشكال هذه الإعتداءات في هذا المجال فنجد ما اصطلح على تسميتها "حصان طروادة" يقع بموجبها تبديل معلومات الحاسب بواسطة برنامج مصغر في برنامج التطبيق لكي يقوم ببعض الوظائف غير المصرح بها في نفس الوقت الذي يقوم فيه هذا الأخير بكل وظائفه الأصلية الأخرى. وتؤدي هذه العملية إذا أدخلت على احدى البرامج الموجهة لمعالجة عدد من الحسابات المالية الى النزول بصنتيم على الحسابات الحقيقية ثم تنضاف كل النسب المخصومة الى حساب شريك له.

كما نجد ما يسمى بتقنية سالامي ، وهي عملية يتم بواسطتها خصم مقادير زهيدة من مجموع أعداد كبيرة من المبالغ بطريقة آلية معقدة بحيث يمكن التفطن بسهولة لكنها في الواقع تدر على مقترفيها أموالا طائلة.

وتجدر الإشارة الى أن هناك العديد من العمليات الأخرى ذات الصبغة التقنية والفنية البحتة التي لا يتسع المجال لشرحها بكل دقة ، مثلما يعرف بطريقة الأبواب المصيدة أو الأبواب الخادعة، وتتمثل في ترك فراغات ومساحات ومنافذ للوصول الى البرامج ليقع استغلالها عند الحاجة وذلك باللجوء الى إضافة برنامج ثانوي.

أ- تطبيقات المعلوماتية

للمعلوماتية عدة تطبيقات تكاد لا تحصى، وهي تمتاز بتطوّرها المطّرد الذّي لا يتوقّف، وما يمكن أن يقال اليوم، قد نتجاوزه في الغد، لكنّها تجتمع على كلمة واحدة وهي أنّها تتأسّس على أنظمة معلوماتيّة. وتشمل على وجه الخصوص ما يعرف ببنوك المعلومات وقواعد البيانات والوسائط المتعدّدة والشّبكات المعلوماتيّة.

-بنوك المعلومات: وهي على رأي توصيّات الاتّحاد الأوروبي " مصنّفات من المعطيات والعناصر المتّصلة بها والمنظّمة بطريقة آليّة ومنهجيّة والتّي يمكن النّفاذ إليها شخصيّا سواء بواسطة الوسائل الإلكترونيّة أو بواسطة وسائل أخرى "،وعرّفها القانون الفرنسي بأنّها " مجموعة من المعطيات الخاصّة بمجال محدّد من المعارف، ومنظّمة بطريقة يسهل استشارتها من الغير ". ويتلخّص من ذلك أنّه من الممكن جمع المعلومات في نشاط معرفي معيّن، على أنّ يتمّ تنظيمها بشكل دقيق ومبسّط، وفي إطار منهجيّة محدّدة، ويمكن بالتّالي لكلّ طرف النّفاذ إلى هذه المعطيات وقضاء حاجته، ومن المفترض أن تكون هذه المعطيات موضوع معالجة إلكترونيّة ومحفوظة بذاكرة الحاسوب، على أن يتحقّق للغير التّوصّل بهذه المعارف كلّما فتح الحاسوب وضغط بالمكان المناسب، ومن الممكن أن تنظّم بنوك المعلومات بأقراص ضوئيّة مكتنزةCDRom أو أقراص رقمية متعدّدة الوسائط D.V.D أو غيرهما، فتوضع هذه الأقراص بموضعها لتفتح، ويتّصل المعني بالمعلومات التّي يريدها، لكنّ الشّئ الهام في ذلك هو أنّه بالإمكان النّفاذ إلى بنوك المعلومات بطريقة إلكترونيّة عن بعد، إذا كانت هذه البنوك مرتبطة بشبكات معلوماتيّة.

-قواعد البيانات: وهي مجموعة من البيانات المنظّمة لغاية استعمالها بواسطة البرامج المعلوماتيّة المناسبة والمميّزة بشكل يسمح بتسهيل التّطوّر المستقلّ للمعطيات والبرامج. أو هي مجموعة الأعمال والمواد المنسّقة والمخزّنة والتّي يمكن الوصول إليها عن طريق وسائل إلكترونيّة بما في ذلك العناصر الضّروريّة

لتشغيل القاعدة. ويرد على رأس قواعد البيانات ما يعرف بالفهارس (répertoires ou annuaires ou indexes).

-الملتيميديا والأنفوميديا: تطوّر عالم المعلوماتيّة بشكل سريع، حيث ارتقت المعالجة الإلكترونيّة، بفضل التّقنيّات الجديدة في عالم البرمجيّات والأنظمة، إلى وسائط متعدّدة الاستعمالات Multimedia سواء كانت في شكلها غير المباشر أي المضمّنة بأقراص ضوئيّة مكتنزة CDRom أو المباشر أي المحالة بواسطة شبكة الأنترنات، وأصبحنا نتحدّث عن الوسائط المعلوماتيّة infomedia. وتعرف الوسائط المتعدّدة بكونها مجموعة التّقنيّات والمنتوجات التّي تسمح باستعمال المعلومات في شكل نصوص أو صور سواء كانت ثابتة أو متحرّكة، وبطريقة تفاعليّة. فهي نتيجة للتراكم التّقني في الرّقمنة numérisation الذّي مكّن من الاستعمال المجتمع للصورة والصّوت والنصّ، وبطريقة تفاعليّة.

وإذا كانت البداية حصرت المعلوماتيّة وخدماتها في مجرّد العمليّات الحسابيّة فإنّ التّطبيق الحالي جعل من تكنولوجيا المعلومات، مفهوما يتّسع إلى جميع المواد والبرمجيّات والخدمات التّي تسمح بمعالجة ونقل المعلومة، بل إنّ نجاح شبكات الاتّصالات الحديثة جعل هذا المفهوم يستوعب التّبادل الإلكتروني للبيانات وشبكة الأنترنات. فهو خلط بين المعالجة الإلكترونيّة والاتّصالات.

-الشّبكات المعلوماتيّة: وتعرف بمجموعة الوسائل الماديّة والبرمجيات المخصّصة للاتّصالات بين الحواسيب والوسائل الطّرفيّة. ويمكن أن تكون شبكات مغلقة أو مفتوحة. وقد أصبحت التطبيقات المغلقة أساس تنظيم المؤسّسات الاقتصادية والإدارية ولعلّ أهمّها ما يعرف بشبكة تونس للتّجارة وشبكة المقاصة الإلكترونيّة. وقد تكون هذه الشبكات المغلقة ونظامها أن لا تستعمل من العامة ولا يصح النفاذ إلى محيطها إلا بالإذن، وعادة ما تكون هذه الشبكات محمية بوسائل فنية تمنع الدخول إليها بدون تسجيل سابق[23].

ب- المتدخلون في المجال المعلوماتي

---

[23] يأتي في هذا الباب التّبادل الإلكتروني للبياناتEchange de données informatisés EDI،وهو اتّفاق مسبق للمبادلات الإلكترونيّة طبق ضوابط معيّنة، يحدّد به محتوى الوثائق موضوع التبادل وكيفيّة ضمان سرّيتها وسلامتها وجميع المسائل التّي لها علاقة بالإثبات والقانون المنطبق، إلى غير ذلك من المسائل الاتّفاقيّة والتّي لها علاقة بالجوانب الإلكترونيّة، ومن تطبيقاته التبادل الإلكتروني للمطبوعات Echange de formulaires informatisés EFI. ويأتي في هذا الباب ما يعرف بالإنترانتIntranet والإكسترانات Extranet. وهي أدوات تقنيّة تتوفّر خاصّة للمؤسّسات الاقتصاديّة لضمان الانتشار والتّحكّم في الموارد. أما الشبكات المفتوحة، فتبقى عامة يصح للجميع الانتفاع بخدماتها، ولعلّ المثال الهام في ذلك هو شبكة الأنترنات، متى أمكن الرّبط المباشر والمفتوح بين الحواسيب المشتّتة هنا وهناك. وكان ذلك سببا في نشأة نظام جديد. ومن ثمّ أمكن تبادل المعلومات بصفة إلكترونيّة وتوفير جملة من الخدمات عن بعد، وبمواصفات معلوماتيّة. فهي مجموعة من آلاف و ملايين المستعملين بدون حدود جغرافية أو ضغوط زمنية، وهي مجموعة غيرمتناهية من المعلومات.

تعمل شبكة الأنترنات من خلال بروتوكولات وهي جملة من القواعد الفنيّة المحدّدة لكيفيّة تنفيذ العمليّات، فهي الطّريقة المعتمدة فنيّا في نقل البيانات وتنظيمها، وهي طريقة نموذجيّة يعتدّ بها على المستوى الدّولي. ويستخلص من ذلك أنّها عبارة عن نظام وصفي للطّريقة الفنيّة المعتمدة في نقل وتنظيم المعلومة، أي جملة الضّوابط التّي من المفروض احترامها لضمان تنظيم المعلومة في مرحلة أولى ونقلها في مرحلة ثانية ثمّ إعادة تنظيمها في مرحلة ثالثة. وهي متعدّدة وتكاد لا تحصى ولا تعدّ، والأغلب أن تكون مفتوحة، بمعنى أنّها معلومة من الكافّة، وبالإمكان استغلالها بدون قيد وللأنترنات عدة تطبيقات.

المتدخّل المقصود هو المتدخّل في إطار التّطبيقات المعلوماتيّة وخدماتها أي استغلال المعلوماتيّة بشكل عام، فيخرج عن ذلك، بطبيعة الحال، جميع المتدخّلين في صناعة المعدّات المعلوماتيّة أو صيانتها أو بيعها أو شرائها أو كرائها أو توريدها أو تصديرها. ويأتي المستعمل أو صاحب المحتوى أوّل المتدخّلين في استغلال المعلوماتيّة، وإذا انتقلت المعلومة من مكان إلى مكان، في إطار الشّبكات المعلوماتيّة، فيفترض أن يتدخّل مزوّد الدّخول ومزوّد النّقل، وتأتي الخدمات ذات القيمة المضافة من نوع أنترنات بعدّة صور جديدة من الخدمات، وتتطلّب إضافة إلى ما تقدّم، تدخّل مزوّد الإيواء ومحرّكات البحث وعدّة هياكل أخرى.

ويتلخّص من ذلك أنّ المتدخّلين بالشّبكة على كثرة، لأنّ عددهم لا يحصى ولا يعدّ، فمنهم من يضمن الربط، ومنهم من يضمن نقل المعلومة، ومنهم من يضمن خدمة الإيواء، أي إيواء المعلومة hébergement، أو البحث عنها recherche، ومنهم من يضمن خدمة المصادقة الإلكترونيّة certification، ومنهم من يضمن علامة المواقع[labellisation، ومنهم من يعرض وسائل التّشفير. ورغم كثرتهم فإنه يمكن ردّهم إلى فئتين، ففئة منهم تتدخل على المستوى الفني في صياغة وتنظيم الأنظمة المعلوماتية وفئة أخرى تساهم في عرض المحتوى المعلوماتي في مجمله على العامّة أو الخاصّة، والمعنيّون بذلك فقط مزوّد الدّخول ومزوّد النّقل ومزوّد الإيواء ومزوّد البحث. معنى ذلك أنّه يخرج من مفهوم المتدخّلين في استغلال المعلوماتيّة صنفان، فمنهم من يستفيد من خدمات المعلوماتيّة، فنسمّيه بالمستفيد والمستعمل، أو ينتج المحتوى فنسمّيه بمزوّد المحتوى، ومنهم من يقوم على تزويد الغير بهذه الخدمات، فنسمّيه بمزوّد الخدمات. وبمعنى آخر هناك من يخلق المحتوى المعلوماتي أو يستفيد منه، وهناك من يعرض هذا المحتوى، وذلك هو المقصود من عبارة المتدخلين في المجال المعلوماتي، وهم من ستلقى عليهم المسؤولية المعلوماتية في نهاية الأمر حسب درجات تدخلهم.

المعلوماتيّة بأنظمتها وبرامجيّاتها أصبحت هيّ الأساس في جانب كبير من الشّبكات والأعمال السمعيّة والبصريّة، فنقول بالشّبكات المعلوماتيّة، كما أنّ الوسائط المتعدّدة ليست إلاّ منتوجا سمعيّا بصريّا، في نهاية الأمر. ورغم هذا التّداخل بين قطاع المعلوماتيّة من جهة والاتّصالات والوسائل السمعيّة البصريّة من جهة أخرى، فإنّ الحدود بينها واضح، وهو أنّ المعلوماتيّة تتعلّق بالأنظمة المعلوماتيّة والبرامجيّات، في حين أنّ الاتّصالات ترتبط بمفهوم الشّبكات، وتشمل الوسائل السّمعيّة البصريّة مجموعة الأصوات والألوان والصّور والألواح الموسيقيّة. ولكنّ الترابط وثيق بين المعلوماتية ومعنى الاتصالات والمصنفات السمعية البصرية إذا انبنت هذه الأخيرة

على أجهزة ومعدات وتنظيمات معلوماتيّة، بل إن التنظيم المفتوح للشبكات تجاوز معنى الاتصالات ليشمل معنى النشر والصحافة وغير ذلك من الخدمات. معنى ذلك أن الحديث عن الأنظمة المعلوماتية والمعطيات الإلكترونية المجردة يحمل إلى تقنيات المعلوماتية بينما الحديث عن خدمات المعلوماتية يحمل إلى المحتوى المعلوماتي، وذلك ما يكون عادة محل الجريمة المعلوماتية التي يمكن أن تشمل في نهاية الأمر ليس المستعمل فقط ومزود المحتوى بل إن الفنيين كذلك يمكن أن تحمل على أوزارهم المسؤولية الجزائية.

الفرع الثاني: تجريم الاعتداء على البرنامج المعلوماتي

النص الجزائي المنطبق في تونس على الجرائم الواقعة على الأنظمة الالكترونية أو المعلوماتية هوالفصل 199 مكرر من المجلة الجزائية الذي أضيف بالقانون عدد 89 لسنة 1994 المؤرخ في 02 أوت 1999.

فالتجريم نص عليه الفصل 199 جديد بالفقرة الأولى منه والذي وإن كان يمثل اعتداء على المعلوماتية الا أن باعثه لا ينبع من الرغبة في الكسب وتحقيق الثراء بخصم المبالغ المالية أو تحويلها ، وإنما ينبع من دوافع التجسس عن برامج ومخططات الآخر باختراق أنظمته للحصول على معلومات أو إرشادات تكون محاطة بالسرية والتحفظ من طرف المؤسسة أو الشخص المالك لها. إذا جاء بالفصل المذكور" يعاقب بالسجن من شهرين إلى عام وبخطية قدرها ألف دينار او بإحدى هاتين العقوبتين فقط كل من ينفذ أو يبقى بصفة غير شرعية بكامل أو جزء من نظام البرمجيات والبيانات المعلوماتية".

وترفع العقوبة الى عامين سجنا والخطية الى ألفي دينار إذا نتج عن ذلك ولو من غير قصد إفساد أو تدمير البيانات الموجودة بالنظام المذكور".

ينص الفصل 199 المذكور على جريمتين وهما **النفاذ** من جهة و**البقاء** من جهة أخرى وذلك بصفة غير شرعية بكامل أو بجزء من نظام البرمجيات والبيانات المعلوماتية.

1) النفاذ: يجرم القانون إقامة اتصال جزئي أو كلي بنظام البرمجيات والبيانات المعلوماتية بصرف النظر عن الإستغلال الفعلي أو التقاط عناصر منه. وتتحقق هذه الوضعية مثلا بتركيب رمز نفاذ تم التحصل عليه إحتيالا أو باستغلال ضعف نظام المراقبة الخ.....

ولكن النفاذ لا يسقط تحت طائلة القانون إلا إذا كان من فعل شخص ليس له الحق في الولوج الى النظام أو ليس له الحق في الولوج اليه بالطريقة التي استعملها.

2) البقاء: فائدة تجريم البقاء بكامل أو بجزء من نظام البرمجيات والبيانات المعلوماتية يمكن أن يقتصر على مجرد القيام بجولة داخله كما يمكن أن يكون عرضة الإعتداء بالقيام بعمليات غير مرخص فيها. وإذا نتج عن ذلك " ولو عن غير قصد إفساد أو تدمير البيانات الموجودة بالنظام المذكور....." ترفع العقوبة الى عامين سجنا والخــطية إلى ألفـــي دينارا (فصل 199 جديد فقرة ثانية).

وترتبط جرائم الاعتداء على الأنظمة المعلوماتيّة والمعطيات الإلكترونية، بنوع جديد من الإجرام المرتبط بوسائل حماية الأنظمة. حيث إنّ جرائم النّفاذ والالتقاط والاعتداءات بأنواعها، لا يمكن أن تطال الأنظمة المعلوماتيّة المحميّة إلاّ إذا تمّ خرق وسائل الحماية المستعملة. لذلك حرص المشرّع التّونسي على تنظيم هذا الجانب، سواء بالقانون عدد 83 لسنة 2000 المتعلّق بالمبادلات والتّجارة الإلكترونية (الفصل 48) أو بالقانون عدد 1 لسنة 2001 المتعلّق بمجلّة الاتّصالات (الفصل87)، وألقى بالمسؤوليّة الجزائيّة على كلّ من:

- استعمل بصفة غير مشروعة عناصر تشفير شخصية متعلقة بإمضاء غيره.
- استعمل أو صنع أو استورد أو صدر أو حاز لأجل البيع أو التوزيع مجانا أو بمقابل أو عرض للبيع أو باع وسائل أو خدمات التشفير أو أدخل تغييرا عليها أو إتلافها دون مراعاة أحكام الأمر المنصوص عليه بالفصل 9 من مجلّة الاتّصالات. ويذكر أنّ المشرّع ضبط شروط وإجراءات استعمال وسائل أو خدمات التّشفير عبر شبكات الاتّصالات وتعاطي الأنشطة ذات العلاقة، تطبيقا لهذا الفصل، بموجب الأمر عدد 2727لسنة 2001 المؤرّخ في 20 نوفمبر 2001 بداية، وأخيرا بموجب الأمر عدد 2639لسنة 2008 المؤرّخ في 21 جويلية []2008.

كما وضع المشرع نصا خاصا بتزوير آداة الدفع الإلكتروني بموجب القانون عدد51 لسنة 2005 حيث إنّ تزوير أداة تحويل إلكتروني أو استعمال أداة تحويل إلكتروني للأموال مزورة مع العلم بذلك وقبول تحويل أموال باستعمال أداة تحويل إلكترونية مزورة مع العلم بذلك يمثل جريمة حسب القانون الجزائي وتصل العقوبة في ذلك إلى عشرة أعوام والخطية بعشرة آلاف دينار، كما أنّ استعمال أداة تحويل إلكتروني دون إذن صاحبها أصبح يمثل عقوبة جزائيّة تصل العقوبة فيها إلى حدّ ثلاث سنوات والخطية بثلاث بثلاثة آلاف دينار[24].

[24]ومن الممكن أن تتوارد الجرائم فيتمّ النّفاذ إلى الأنظمة المحميّة بواسطة استعمال وسائل تشفير على ملك الغير، ومن الممكن كذلك أن تلحق بالمتّهم جرائم الاعتداء على الأنظمة المعلوماتيّة والمعطيات الإلكترونية والجرائم المتعلّقة بوسائل التّشفير بدون ضمّ، خاصّة إذا لم يحترم المتّهم الذّي نفذ إلى الأنظمة المعلوماتيّة موجبات المصادقة على وسائل التّشفير على سبيل المثال.

ويذكر أنّ المشرّع التّونسي نقل أحكام القانون الفرنسي عدد 19 لسنة 1988المؤرّخ في 5 جانفي 1988 المتعلّق بالتّزوير المعلوماتي في صياغته لأحكام الفصل199 مكرّر والفصل 199 ثالثا والفصل 172 فقرة أخيرة من المجلّة الجزائيّة، لكنّه لم يحافظ على صياغة هذا النّص، كما أنّ الأحكام الواردة بالقانون الفرنسي قد تجاوزها التّطبيق بعض الشيء بشكل أضرّ بالمفاهيم المعتمدة بالقانون التّونسي. فالنّصّ الفرنسي اعتمد مسألة النّفاذ والبقاء وتدمير وفساد المعطيات والاعتداء على نظام المعالجة الإلكترونية وإدخال بيانات وتزوير وثائق إلكترونيّة واستعمالها بأيّة طريقة كانت. غير أنّ المشرّع التّونسي أبقى على جريمة البقاء والنّفاذ والفساد والتّدمير والاعتداء على النّظام وإدخال بيانات، ولم يعتمد المفهوم العام في تزوير الوثائق واستعمالها واقتصر على ذكر " تغيير وثيقة إلكترونيّة أصلها صحيح " تماشيا مع بعض الصّور الخاصّة الواردة بالمجلّة الجزائيّة، الأمر الذّي لم يكن متناسقا بالمرّة مع ما تتطلّبه الإعلاميّة ويُبقي على جملة من الجرائم خارج إطار التّجريم، كما إذا صنع الجاني وثيقة جديدة بعد اطّلاعه على وثيقة تابعة للغير واستعملها في شكلها الجديد دون أن تأتي تحت طائلة الفصل 172 فقرة أخيرة م.ج حيث ولئن نصت هذه الفقرة على "صنع وثيقة مكذوبة أو تغيير متعمّد للحقيقة بأيّ وسيلة كانت في كلّ سند سواء كان ماديّا أو غير ماديّ من وثيقة معلوماتيّة أو إلكترونيّة وميكروفيلم وميكروفيش ويكون موضوعه إثبات حقّ أو واقعة منتجة لآثار قانونيّة" فإن شرط الصناعة والإحداث بالفصل 172 م.ج يتعلق بالوثائق المثبتة للحقوق أي الوثائق التي تتضمن التزاما في نهاية الأمر وليس مجرد رخصة. أما ما كان في باب الفصول 193 إلى 199 ثالثا فمرده لافتعال واستعمال الرخص التي تخرج عن طبيعة الوثائق المقصودة بالفصل 172 م.ج، ولكن الفصل 199 ثالثا لم يورد معنى الصنع والإحداث، وقد عبّر المشرّع الفرنسي على هذه الحالة بقوله " كلّ شخص عمد إلى تزوير وثائق معلوماتيّة مهما كانت طبيعتها من شأنها إلحاق الضّرر بالغير يعاقب ....." ويعاقب كذلك " كلّ من استعمل هذه الوثائق المزوّرة...". وبذلك غفل التنقيح الجديد عن ذكر فعل الصنع بالفصل 199 ثالثا م.ج، كما أنّ التنقيح الجديد لم يبرز حقيقة الاختلاف بين الوثائق الواردة بالفصل 199 ثالثا م.ج والأخرى المنصوص عليها بالفصل 172 فقرة ثالثة ولوأنه من الممكن الوصول إلى بيان الاختلاف، كما فعلنا، رجوعا للسوابق[25]

[25]وينتقد هذا التّشريع الجديد كذلك في حدود أنّه لم يعتمد تعريفات واضحة للمفاهيم التّي استعملها والحال أنّها تمثّل الأساس في ضبط الرّكن المادي للجريمة، حيث استعمل المشرّع التّونسي بالفصل 199 مكرّر مفاهيم لا يتّفق حولها المختصّون للدّلالة على نظام المعالجة الآليّة للبيانات: système de traitement automatisé de données فتبنّى من جهة مفهوم " نظام البرمجيّات والبيانات المعلوماتيّة "، ومن جهة أخرى " نظام معالجة معلوماتيّة "، والحال أنّه لم يتعرّض للفرق بين المفهومين، ولا أظنّ أنّ المشرّع يفرّق بين المفاهيم المستعملة، خاصّة وأنّ النّص الفرنسي للفصل 199 مكرّر تبنّى مفهوما تقنيّا واحدا وهو: نظام المعالجة الآليّة للبيانات. وكان من المؤمّل أن يخيّر المشرّع التّونسي هذا التّوجّه السّليم.

.

واستعمل المشرّع التّونسي بالفصل 199 ثالثا عبارة الوثائق الإلكترونية أو المعلوماتيّة والحال أنّه لا وجود لفرق بين الوثيقة الإلكترونية والمعلوماتيّة. كما أنّ المشرّع التّونسي تبنّى مفهوم المعالجة المعلوماتيّة الذّي لا يتجاوز من الوجهة الواقعيّة نظم المعلوماتيّة التّي لا ترتبط بشبكة مواصلات، وقد تقرّر منذ مدّة وبعد نقاشات متواصلة تطبيق الجريمة الإعلاميّة حتّى بالنسبة إلى نظام تبادل المعطيات الإلكترونية وهو ما يعرف بالالتقاط البيني. لذلك كان من المستحسن لو تبنّى المشرّع التّونسي مفهوم نظام المعالجة الآليّة للبيانات لأنّه مفهوم عامّ يشمل جملة الصّور التّي مثّلت محور النّقاشات الفقهيّة والقضائيّة.

وإذا كان من الجائز تبرير ما أقدم عليه المشرّع التّونسي، فنقول إنّ المشرّع التّونسي تخلّى عن مفهوم نظام المعالجة الآليّة للبيانات بعلّة حرصه على التّفرقة الواضحة بين الاعتداء على البيانات ذاتها بالاطّلاع عليها أو إتلافها أو سرقتها بدون حقّ من جهة، والاعتداء على نظام المعالجة ذاته بتعطيله أو تحويره، وكان ذلك واضحا في إشارة المشرّع إلى نظام البرمجيّات من جهة والبيانات المعلوماتيّة من جهة أخرى. لكنّه كان يخيّر اعتماد المفهوم الفنيّ السّليم للإشارة إلى جملة الصّور والحالات، وهو نظام المعالجة الآليّة للبيانات. ومن هذه النّاحية كان من الضّروري التّدخّل لتنقيح الفصول 172 و199مكرّر وثالثا.

والفائدة من جميع ذلك أن يقع التمييز بعناية بين جرائم الاعتداء على نظام المعالجة الإلكترونية بما في ذلك جرائم التدليس الإلكتروني وهو ما يحمل إلى وقوع الجريمة على ذات السند الإلكتروني صنعا وتغييرا ونفاذا وبين أن تستعمل المعلوماتية كوسيلة في الإجرام، فهي بذلك ليست محلّ الاعتداء وإنما وسيلته فتدخل في معنى الركن المادي المتمّم للجريمة. وإذا كان المشرع اكتفى في بعض الصور بإخضاع الإجرام المعلوماتي إلى التشريع الجاري به العمل دون إشارة إلى وسيلة المعلوماتية،

يراجع مقال بالأنترنت للقاضي الدكتور على كحلون بعنوان الجريمة المعلوماتية.