الوقاية من تزوير بطاقات الدفع الالكترونية كآلية للحد من الفساد المالي في البنوك والمؤسسات المالية

_ حالة فرنسا_

شايب محمد
أستاذ مساعد بكلية العلوم الاقتصادية والتسيير والعلوم التجارية
جامعة سطيف / **الجزائر**

بارك نعيمة
أستاذ مساعد بكلية العلوم الاقتصادية والتسيير والعلوم التجارية
جامعة الشلف / **الجزائر**

ملخص:

انتبهت السلطات المالية في الدول المتقدمة مؤخرا إلى تزايد خطر عمليات النصب والاحتيال عن طريق تزوير بطاقات الائتمان الالكترونية، وفي هذا الإطار انطلقت حملات حول الاستعمال الأفضل للبطاقات البنكية وتحسيس مختلف الناشطين بأهمية الوقاية من مخاطر التدليس في مجال النقديات، وهي الحملة التي تهم مختلف الجهات والمناطق والأفراد والمؤسسات، وتؤكد جميع المؤشرات أن الجرائم الإلكترونية من خلال بطاقات الدفع مرشحة للارتفاع من سنة إلى أخرى كما هو الحال في فرنسا.

Abstract *:*

Lately, the financial authorities in the developed countries realized the threat posed by the incresing fraud and embezzlement's operations through the falsification of the elecronic credit cards. Apparently, a huge range of campaigns were launched concerning the best use of those credit cards and rise the awareness of the different stakeholders of the importace of prevention from the frauding risks in the currency field. And this campaign concerns the various entities, regions, individuals and institutes. And all the indicators confirm that the elecronic crimes through the credit cards are expected to rise from year to year as the case in France.

مقدمة:

إن للمؤسسات المالية أنشطة عديدة ومتنوعة تعتمد في تأديتها على موارد مختلفة، ومن أبرزها الموارد المالية، هذه الأخيرة من أكثر الموارد التي تتعرض للمخاطر ومن أهمها مخاطر الفساد المالي الذي يحمل في طياته العديد من الآثار السلبية المؤثرة على أنشطة المؤسسات المالية.

تعطي البنوك والمؤسسات المالية أهمية كبيرة لمكافحة الفساد المالي ومن أشكاله تبييض الأموال. وهذا يأتي ضمن أبرز أولوياته الهادفة إلى تأمين سلامة ومتانة القطاع المالي والمصرفي في الاقتصاد. ومع التطور التكنولوجي أجبرت البنوك والمؤسسات المالية غلى تبني تكنولوجات الاعلام والاتصال الحديثة، لكن هذه الأخيرة فبالرغم من ايجابياتها في تأثيرها على النشاط المالي الا انها احدثت نوعا جديدا من المخاطر سميت بالجرائم الالكترونية.

لقد صاحب انتشار بطاقة الدفع الإلكتروني، وتزايد حجم التعامل بها، نمواً مضطرداً في الجرائم المصاحبة لها، واستخدامها بطريقة غير مشروعة، حيث احترف بعض الافراد في تزوير هذه البطاقات، أو سرقتها لاستخدامها في الاستيلاء على مال الغير، ونظراً للخسائر الفادحة المترتبة على ظاهرة الاستخدام غير المشروع، فقد أصبح يطلق عليها جريمة العصر، كما أنّها تعد فرصة كبيرة لغاسلي الأموال.

– أهمية الموضوع: تشير المصادر من الأوساط المالية إلى أن المبالغ المالية الضائعة بسبب التدليس في بطاقات الائتمان يقدر بالملايير، مؤكدة صعوبة تحديد هذه المبالغ، نظرا لتكتم الجهات المتضررة حول الموضوع، وراح ضحيتها مواطنون ومراكز تجارية ووحدات سياحية وبنوك ومؤسسات مالية. فرنسا هي كذلك تحاول جاهدة تدريب عناصر قوى الأمن الداخلي لحماية عمليات الدفع والسحب الالكتروني بصفة خاصة وفي مجال الجرائم المنظمة خصوصا تبييض الأموال والجرائم المالية بصفة عامة.

من خلال ما سبق يمكن طرح الإشكالية التالية:

كيف يمكن للبنوك والمؤسسات المالية الوقاية من تزوير البطاقات الالكترونية من أجل الحد من الغش والفساد المالي ؟

– أسباب احتيار الموضوع: يعود أسباب اختيارنا للموضوع إلى:

– أهمية الموضوع كونه الشغل الشاغل مؤخرا بالنسبة للمؤسسات المالية العالمية خاصة في الدول المتقدمة بفعل تزايد عدد الجرائم الالكترونية من خلال لهذه البطاقات.

– الأهمية الكبيرة لموضوع مكافحة الجرائم المالية ولكل شكل من أشكال المساس بالأموال العامة واموال جمهور عملاء البنوك والمؤسسات المالية.

ـ الجزائر في خضم تحديثها لنظام دفعها الالكتروني هي مقبلة على استخدام كل أشكال البطاقات الالكترونية شيئا فشيئا، مما ينبغي التطرق لآليات هذه البطاقات وكذلك ايجابياتها وسلبياتها.

ـ شيوع الخبر المتداول مؤخرا حول تداول بطاقات مغناطيسية مزورة، لسحب الأموال عبر مختلف الموزعات الآلية، حيث تقوم شبكات مجهولة بترويجها بعد سرقة الأرقام السرية من أصحاب البطاقات من أجل استخدامها وسحب أموال المواطنين من أرصدتهم. لذا قررنا توضيح مختلف عمليات التزوير والتدليس الممكن قيام بها من خلال البطاقات المغناطيسية.

لمعالجة هذا الموضوع وللإجابة عن الإشكالية سوف نتطرق إلى المحاور التالية.

ـ **المحور الأول:** الفساد المالي وظاهرة غسيل الأموال.
ـ **المحور الثاني:** بطاقات النقد الالكتروني وأنواعها.
ـ **المحور الثالث:** الدفع الالكتروني بالبطاقة المغناطيسية وطرق وآليات الغش فيها.
ـ **المحور الرابع:** طرق الغش والجرائم المختلفة باستخدام البطاقة الالكترونية في فرنسا.
ـ **المحور الخامس:** كيفية الوقاية من الظاهرة تزوير البطاقات الالكترونية.
ـ **المحور السادس:** تزوير بطاقات السحب البريدية والبنكية الجزائرية.

المحور الأول: الفساد المالي وظاهرة غسيل الأموال

للمؤسسات المالية أنشطة عديدة ومتنوعة تعتمد في تأديتها على موارد مختلفة ومن أبرزها الموارد المالية، ويعد هذا المورد من أكثر الموارد التي تتعرض للمخاطر ومن أهمها الفساد المالي الذي يحمل في طياته العديد من الاثار السلبية المؤثرة على انشطة المؤسسات المالية.

أولا– الفساد المالي مفهومه، مظاهره أسبابه: سنحاول فيما يلي التطرق لمفهوم ومظاهر وأسباب الفساد المالي:

1– تعريف الفساد المالي: يتمثل في الانحرافات المالية ومخالفة القواعد والأحكام المالية،ويعرف بأنه كافة المخالفات للقواعد المالية التي تنظم سير العمل المالي لمؤسسات المالية، وكذا مخالفة التعليمات الخاصة بأجهزة الرقابة المالية [1]، ومن التعاريف السابقة يمكن تعريف الفساد المالي بأنه كافة التجاوزات التي تمس الجانب المالي فقط من المؤسسات المالية.

2- مظاهر الفساد المالي: تتمثل فيما يلي[2]:

– الرشوة: وتعني حصول الشخص على منفعة تكون مالية في الغالب لتمرير أو تنفيذ إعمال خلاف التشريع أو أصول المهنة

– **المحسوبية:** أي إمرار ما تريده التنظيمات (الأحزاب أو المناطق والأقاليم أو العوائل المتنفذة) من خلال نفوذهم دون استحقاقهم لها أصلاً.

– المحاباة: أي تفضيل جهة على أخرى بغير وجه حق كما في منح المقاولات والعطاءات أو عقود الاستئجار والاستثمار.

– **الوساطة:** أي تدخل شخص ذا مركز (وظيفي أو تنظيم سياسي) لصالح من لا يستحق التعيين أو إحالة العقد أو إشغال المنصب أو ...

– الابتزاز والتزوير: لغرض الحصول على المال من الأشخاص مستغلاً موقعه الوظيفي بتبريرات قانونية أو إدارية أو إخفاء التعليمات النافذة على الأشخاص المعنيين كما يحدث في دوائر الضريبة أو تزوير الشهادة الدراسية أو تزوير النقود والبطاقات الالكترونية في حالة الدفع الالكتروني.

– نهب المال العام: والسوق السوداء والتهريب باستخدام الصلاحيات الممنوحة للشخص أو الاحتيال أو استغلال الموقع الوظيفي للتصرف بأموال الدولة بشكل سري من غير وجه حق أو تمرير السلع عبر منافذ السوق السوداء أو تهريب الثروة النفطية.

– فساد يتقاطع مع الأنظمة والقوانين المتعلقة بنظام العدالة وحقوق الملكية والتسهيلات المصرفية والائتمانات وكذلك التمويل الخارجي.

3- أسباب الفساد المالي: تتمثل في الآتي [3]:

- **أسباب سياسية:** ويقصد بالأسباب السياسية هي غياب الحريات والنظام الديمقراطي، ضمن مؤسسات المجتمع المدني، ضعف الأعلام والرقابة.
- **أسباب اجتماعية:** متمثلة بالحروب وأثارها ونتائجها في المجتمع والتدخلات الخارجية، الطائفية والعشائرية والمحسوبيات القلق الناجم من عدم الاستقرار من الأوضاع والتخوف من المجهول القادم ... جمع المال بأي وسيلة لمواجهة هذا المستقبل والمجهول الغامض.
- **أسباب اقتصادية:** الأوضاع الاقتصادية المتردية والمحفزة لسلوك الفساد وكذلك ارتفاع تكاليف المعيشة.
- **أسباب إدارية وتنظيمية:** وتتمثل في الإجراءات المعقدة (البيروقراطية وغموض التشريعات وتعددها أو عدم العمل بها)، وضمن المؤسسة لعدم اعتمادها على الكفاءات الجيدة في كافة الجوانب الإدارية.
- وقد حدد البنك الدولي مجموعة من الأسباب لظهور الفساد المالي والإداري أبرزها ما يأتي:

- تهميش دور المؤسسات الرقابية، وقد تكون تعاني من الفساد هي نفسها.
- وجود البيروقراطية في مؤسسات الدولة.
- حصول فراغ في السلطة السياسية ربما بسبب الصراع علي السلطة.
- ضعف مؤسسات المجتمع المدني وتهميش دورها.
- توفر البيئة الاجتماعية والسياسية الملائمة لظهور الفساد.

ثانيا– ظاهرة غسيل الأموال: ترجع عمليات غسل الأموال بوسائلها الحديثة إلى سنة 1932 حيث بوشرت بشكل منظم بواسطة شخص يدعى Meyer Lansky كان يمثل حلقة الوصل بين المافيا الأمريكية والمافيا الإيطالية خلال الحرب العالمية الثانية وذلك لتسهيل دخول القوات البحرية للحفاء جزيرة صقلية ومن أجل ذلك تم اللجوء إلى البنوك السويسرية من أجل إخراج النقود من الولايات المتحدة الأمريكية وإيداعها في بنوك بسويسرا من خلال قروض وهمية وبفضل هذه الأموال المعاد توجيهها استطاع إقامة مدينة لألعاب القمار في Las Vegas الأمريكية [4].

1- تعريف غسيل الأموال: غسل الأموال تنصب على أموال غير مشروعة يطلق عليها المال القذر وهذه الأموال تختلف عن الأموال السوداء التي تتسم بمشروعية مصدرها إلا انه يتم الاحتفاظ بها سراً للتهرب من الضرائب على الدخل [5].

وعرفته اللجنة الأوروبية لمكافحة غسيل الأموال بأنه: عملية تحويل الأموال المتحصلة من أنشطة إجرامية بهدف إنكار أو إخفاء المصدر الأصلي غير الشرعي لهذه الأموال، أو مساعدة أي شخص ارتكب جرمًا ليتجنب المسؤولية القانونية عن الاحتفاظ بمتحصلات هذا الجرم.يقصد به أيضا إخفاء حقيقة الأموال المستمدة من طريق غير مشروع عن طريق القيام بتصديرها أو إيداعها في مصارف دول أخرى أو نقل إيداعها أو توظيفها أو استثمارها في أنشطة مشروعة للإفلات بها من الضبط والمصادرة وإظهارها كما لو كانت مستمدة من مصادر مشرعة [6].

2– خصائص غسيل الأموال: يمكن إبراز خصائصها فيما يلي [7]:

- أنها جريمة عالمية لا ترتكز في إطار الدولة فحسب.
- جريمة مدروسة ومنظمة بإتقان.
- ضخامة المبالغ التي يتم التعامل بها.

وهناك خصائص أخرى تتمثل في[8]:

- عملية غسيل الأموال تعد نشاطا مكملا لنشاط رئيسي سابق مثل الرشوة والاحتيال والاتجار بالمخدرات...
- سرعة الاتصال والانتقال أوجدت شكلا جديدا من الجرائم منها جريمة غسل الأموال.
- عملية غسل الأموال لم تعد أحادية الجانب في تحركاتها وأصبحت تكتسب أبعاد دولية بعد أن كانت محلية فقط.

المحور الثاني: بطاقات النقد الالكتروني وأنواعها

إن الانتشار الواسع لأنظمة الدفع الالكترونية يترجم المزايا والراحة التي توفرها للعملاء، فلهذه الأنظمة ايجابيات وخصائص تميزها عن الأنظمة التقليدية وتجعل البعض يفضلها عنها. وبطاقات الدفع باعتبارها أهم وأشهر الوسائل الالكترونية للدفع لها ما يميزها عن تلك الوسائل التقليدية والتي يمكن تلخيصها كما يلي:

أولا– أساسيات في بطاقات الائتمان:

1- نشأة البطاقة المغناطيسية: وقد بدأ استخدام البطاقات البنكيّة في منتصف القرن السابق تقريبا، حيث لم يكن الهدف من البطاقة آنذاك إلا الدعاية والمنافسة بين المحلات التجاريّة وتسهيل عمليّة البيع بالثمن المؤجّل أو المقسّط. وكانت العلاقة بين مصدر البطاقة (المحلّ) ومستخدم البطاقة علاقة ثنائيّة فقط، وكانت بطاقة شركة دينارز كلوب Diners Club البداية الحقيقيّة لما نعرفه اليوم من بطاقات. وتعني نادي الطاعمين وكان ذلك سنة 1949 [9]، وكانت الفكرة الأساسية من البطاقة أن تقوم الشركة بدور الوسيط المالي بين البائع والمشتري حامل البطاقة، وذلك بأن تدفع عن المشتري قيمة البضاعة أو الخدمة التي اشتراها (بعد خصم عمولة يسيرة) ثمّ ترسل للمشتري فاتورة بالمبلغ بعد مدّة محدّدة فيدفع المشتري كلّ المبلغ. وقد لقيت البطاقة قبولا واسعا جعلها محلّ نظر البنوك التجاريّة التي تريد أن تستفيد من الفكرة.

2- تعريف بطاقات الائتمان Credit Cards: هي إحدى أنواع بطاقات المعاملات المالية، وهي من البطاقات القرضية التي تتيح لصاحبها الحصول على الائتمان، وهذا الائتمان قد يكون في شكل سلع أو خدمات أو نقود أو في شكل آخر له قيمة مالية. هذه البطاقة تمثل ائتمانا حقيقيا لحامل البطاقة ويطلق عليها أيضا في فرنسا Accréditive la Carte، حيث يتمتع حاملها بائتمان فعلي من البنك المصدر لها ولا يلزم بالوفاء فورا بالسداد [10].

3- أنواع بطاقات الائتمان: وهناك عدة أنواع وإصدارات لبطاقات الائتمان، أهمها[11]:

– بطاقة فيزا Visa Card: تصدر عن منظمة فيزا العالمية، وهذه البطاقة هي بطاقة متجددة بإمكان حاملها أن يسدد التزامات البطاقة أو جزءا منها خلال مدة السماح وأن يسدد الباقي بعد ذلك. موقعها على شبكة الانترنت كالتالي: www.visa.com

– ماستركارد Master Card: تأتي في المنزلة الثانية بعد بطاقة فيزا من حيث درجة انتشارها، فهي أيضا تتعامل مع ملايين المؤسسات والمحلات التجارية، وهذه البطاقة هي أيضا بطاقة متجددة ولها عدة أشكال، ماستركارد: الفضية، الذهبية، المدنية ورجال الأعمال. موقعها على شبكة الإنترنت كالتالي: www.mastercard.Com

– بطاقة أمريكان اكسبريس American Express: وهي بطاقة ائتماني لكنها غير متجددة، فهي ليس لها حد صرف، والمبلغ الكلي المحمل على البطاقة يكون مستحقا عند نهاية فترة السداد، أي ينبغي تسديد الالتزامات المادية لهذه البطاقة خلال مدة السماح[12]. وبخلاف ذلك فإنه لن يجري تجديد هذه البطاقة لمدة جديدة، وهي أنواع (الخضراء، الذهبية،

الماسية)، وكل نوع من الأنواع المذكورة يمنح لقطاع معين من الزبائن المستفيدين. موقعها على شبكة الانترنت كالتالي: www.americanexpress.com

– **بطاقة دينرز كليب** Diners Club Card: إذ يشترط في استمرارها لمدة سماح جديدة تسديد التزاماتها خلال مدة السماح، حملة هذه البطاقة بالملايين لكنهم أقل من حملة البطاقات السابقة. موقعها على شبكة الإنترنت كالتالي: www.dinersclub.com

4- أطراف التعامل في بطاقات الائتمان: إن أطراف التعامل في بطاقة الائتمان هم بشكل عام [13]:

– **المركز العالمي للبطاقة:** كمؤسسة عالمية تتولى إنشاء البطاقة ورعايتها والموافقة على عضوية البنوك في جميع أنحاء العالم للمشاركة في إصدارها وتسوية المستحقات المالية بينهم، والقيام بدور المحكم لحل أي نزاعات تنشأ بين المتعاملين بالبطاقة.

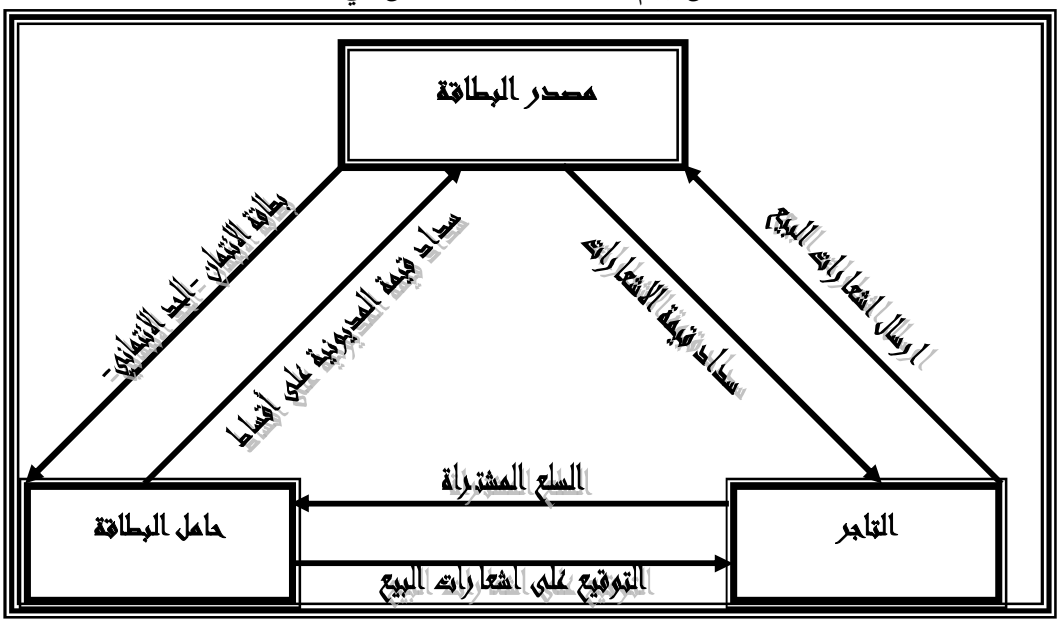
– **مصدر البطاقة:** جميع البنوك المنتشرة في جميع أنحاء العالم، تقوم بالترويج للبطاقة لدى الأفراد للحصول عليها، ودفع مستحقات التجار على حملة البطاقات الصادرة منهم.

– **التاجر:** وهو اصطلاح يطلق على الشركات والمؤسسات التي يتم اتفاق المصدر معها على قبول البيع لحامل البطاقة، ثم الرجوع على المصدر بالثمن المستحق.

– **حملة البطاقات:** وهم الأفراد الذين يوافق المصدر على طلبهم بالحصول على البطاقة لاستخدامها في الحصول على السلع والخدمات من التجار بمجرد تقديم البطاقة، أو سحب نقدية من آلات السحب النقدي أو البنوك وفروعها المشتركة في عضوية البطاقة، ثم دفع المستحقات للبنك المصدر حسب نوع البطاقة.

ومن الناحية التعاقدية، فإنه يمكن النظر إلى المركز العالمي للبطاقة والمصدر المحلي كطرف واحد، لأن التزاماتهم وحقوقهم اتجاه الطرفين الأخيرين واحدة، وبالتالي فإنه من الناحية التعاقدية يوجد ثلاثة أطراف، مصدر البطاقة، التاجر وحامل البطاقة. والشكل التالي يوضح أطراف التعامل بالبطاقة والعلاقة بينهم:

الشكل رقم (01): أطراف التعامل في بطاقة الائتمان



المصدر: عبد الهادي النجار، **بطاقات الائتمان والعمليات المصرفية الالكترونية**، أعمال المؤتمر العلمي السنوي لكلية الحقوق بجامعة بيروت العربية- أعمال المصارف من الوجهتين القانونية والاقتصادية-، منشورات الحلبي الحقوقية، بيروت، لبنان، 2002، ص 39.

ثانيا : بطاقات الخصم الفوري Direct Debit Cards:

1- مفهوم بطاقة الخصم الفوري: يعتبر هذا النوع من البطاقات أوسع البطاقات انتشارا في العالم، لأنه يقلل من مخاطر الديون المعدومة لدى البنوك المصدرة للبطاقات، وإصدارها يتطلب أن يقوم حامل البطاقة بفتح حساب جاري لدى البنك المصدر للبطاقة، ويودع فيه مبلغا من المال لا يقل رصيده عن الحد الأقصى المسموح له بالشراء في حدوده. ويوجد لدى التاجر جهاز خاص متصل بمركز البطاقات لدى البنك (المصدر للبطاقة).

2- **التعامل بالبطاقة**: تمرر البطاقة في الجهاز فيتم قراءة بياناتها من خلال الشريط الممغنط الموجود خلف البطاقة، ويتم الاتصال بمركز البطاقات آليا ثم يتم الاتصال بالفرع المفتوح لديه الحساب ويتم الاطلاع على رصيد الحساب، وإذا كان هذا الأخير يسمح بالخصم فتتم العملية آليا، أما إذا كان الرصيد لا يسمح، فسيتم ظهور ذلك على الجهاز بما يفيد عدم إتمام العملية ليتم إلغاؤها [14].

كما يظهر فإن هذه البطاقة لا تتضمن في جوهرها ائتمانا مقدما من البنك وإنما تسمح لحاملها بأن يحصل على سيولة أو يستخدمها في تسوية مدفوعاته وذلك في حدود رصيده الدائن _ دون أي تجاوز_ في حسابه لدى البنك مصدر البطاقة.

3- وفاء البطاقة: وتحتل هذه البطاقة والتي يطلق عليها أيضا بطاقة الوفاء La Carte de Paiement أعلى درجات الضمان للتاجر الذي يقبل الوفاء بها، حيث يلتزم البنك مصدرها بالوفاء، فهي تؤدي وظيفة الشيك المعتمد من البنك المصدر لضمان الوفاء لحامله [15].

ثالثا– بطاقة القيمة المختزنة Stored-Value Card[16]:

1– مفهوم بطاقة القيمة المختزنة: تدعى أيضا البطاقة سابقة الدفع وتختلف عن بطاقة الخصم وبطاقة الائتمان في أنها تحمل قيمة نقدية محددة (كمية ثابتة لرقم النقدية Digital Cash) تدفع مقدما في مقابل الحصول عليها باستخدامها في تسوية المدفوعات الخاصة بالمبلغ والخدمات المشتراة، إذا قاربت قيمة البطاقة على الانتهاء فإنه بالإمكان تخزين قيمة نقد إضافية في البطاقة. وهناك بعض بطاقات القيمة المخزنة المغلقة قابلة للرمي، ولكن حاليا فإن بعض البنوك والمصدرين يصدرون بطاقات قابلة للاستعمال أكثر من مرة وتسمى بأنظمة القيمة المخزنة المفتوحة [17].

2 – مميزات لطاقة القيمة المختزنة: تتميز هذه البطاقة في كونها تتيح للعملاء استخدامها في وجود المبلغ المودع بالبطاقة فقط، ويمكن تكرار ذلك بزيادة قيمة البطاقة. ومن أشهر استخدامات هذه البطاقة بطاقة الهاتف Téléphone Card وبطاقة النقل Transit Card.

رابعا– البطاقة الذكية Smart Card: سنحاول فيما يلي التطرق لتعريف ومميزات البطاقة الالكترونية.

1– تعريف البطاقة الذكية [18]: هي بطاقة تشبه البطاقات الائتمانية في حجمها وشكلها (بطاقة بلاستيكية)، وتحوي على شرائح الكترونية ذات دوائر متكاملة تعمل على تخزين ومعالجة البيانات، كما تعبر عن قيمة نقدية مخزونة ومدفوعة مقدما [19]. هذه البطاقة ابتكرت للتغلب على المشاكل التي تتعلق بالسرية والأمان في بطاقة الائتمان والخصم.

2– أهم مميزات البطاقة الذكية: تتميز البطاقة الذكية عن البطاقات التقليدية بما يلي[20]:

– بطاقة الائتمان لا تحتوي نقدا وهي تحتوي فقط على رقم حساب يمكن تحميله، والبطاقة الذكية يمكنها تخزين أكثر من 100 ضعف من المعلومات أكثر من بطاقة بلاستيكية بشريط مغناطيسي؛

– تحوي البطاقة الذكية للمستخدم على المعلومات الخاصة به، مثل (الحقائق المالية، مفتاح الشفرة الخاصة، معلومات الحساب، أرقام بطاقة الائتمان، معلومات التأمين الصحي والضمان الاجتماعي)، أو أية بيانات أخرى تضاف بالاتفاق بين المؤسسات ذات العلاقة.

– تمثل البطاقة الذكية أفضل حماية ضد إساءة الاستخدام عن بطاقات الائتمان التقليدية، وذلك لأن المعلومات التي توجد عليها مشفرة، وبالتالي فإن سرقة الائتمان غير ممكنة عمليا لأن مفتاح فتح المعلومات المشفرة مطلوب.

3- **تعاملات البطاقة:** من خلال البطاقة الذكية يمكن تحويل النقود منها أو إليها سواء من حساب صاحب البطاقة نفسه أو حساب غيره، وذلك باستخدام الحاسب الشخصي أو أجهزة الصرف الآلي ATM المجهزة لذلك، أو من أجهزة الهاتف المحمول المجهزة لأداء هذه الخدمة، وتجدر الإشارة إلى أن البطاقات الذكية بدأت في الظهور في الولايات المتحدة الأمريكية [21]. يطلق أحيانا على البطاقة الذكية مصطلح "**المحفظة الالكترونية**".

خامسا– المحفظة الالكترونية Electronic Wallet:

1– مفهوم المحفظة الالكترونية: عبارة عن تطبيق الكتروني يقوم على أساس ترتيب وتنظيم آلية جميع الحركات المالية، وتحتوي تلك المحفظة على جميع بيانات المستخدم لتلك البطاقة بصيغة مشفرة Encrypted ويتم تثبيتها على

الكمبيوتر الشخصي أو تخزينها على أحد الأقراص المرنة أو أي أداة يمكن عن طريقها حفظ تلك البيانات واستخدامها للدفع عن طريق شبكة الانترنت في جميع حالات الشراء. وفي ظل الاستخدام اليومي لعمليات الشراء المحلية والعالمية أصبحت الحاجة ملحة جدا لاستخدام تلك التقنية لما لها من سهولة التواصل في الانترنت وما يترتب عليها من تسهيل لعمليات الشراء التي تحتوي في مضمونها تحويلات نقدية صغيرة كانت أم كبيرة وسرعة وصولها للطرف الآخر في ظل التكنولوجيا المتقدمة [22]. وهي أيضا عبارة عن مجموعة من أدلة إلكترونية يجمعها ويقوم بإدارتها من قبل المستخدم على شبكة الانترنت. وقد تتضمن هذه الأدلة الإلكترونية نص تم إدخاله، وملفات إلكترونية، ويسمح وضعها على الإنترنت بتطوير محتوياتها بشكل ديناميكي مع مرور الزمن [23].

2- حلول المحافظ الالكترونية: من بين المشاكل التي تحلها المحافظ الالكترونية [24] هي توفير مكان تخزين آمن بالنسبة لبيانات بطاقة الائتمان والنقد الالكتروني، وتوفر الوقت في الشراء على الانترنيت لأنه يجب كتابة نفس بيانات بطاقة الائتمان وبيانات أخرى كالاسم والعنوان ورقم الهاتف وأشياء أخرى في كل مرة يراد فيها الشراء. وباستخدام حافظة النقود الالكترونية يتم كتابة البيانات مرة واحدة، ويتم إرسال البيانات أوتوماتيكيا للموقع الذي تتم زيارته، وقد تكون المحفظة الالكترونية بطاقة ذكية يمكن تثبيتها على الكمبيوتر الشخصي أو تكون قرصا مضغوطا يمكن إدخاله في فتحة القرص المرن للحاسب الشخصي، ليتم نقل القيمة المالية منه أو إليه عبر الإنترنت [25].

3- معاملات المحفظة الالكترونية: كما يمكن القول أن المحافظ الالكترونية مفيدة بصفة خاصة وتوفر قدرا كبيرا من الوقت، لكن السؤال الذي يثار هو: ما هي المعاملات التي تجريها المحفظة الإلكترونية بالضبط كحد أدنى؟

تخزن المحفظة الالكترونية معلومات الشحن والفواتير شاكلة أسماء المستهلكين (الأولى والأخيرة) وعنوان الشارع والمدينة والولاية والدولة والرقم البريدي ومعظم المحافظ الالكترونية يمكنها أن تحمل أسماء وأرقام بطاقات الائتمان. بما يقدم للمستهلك خيار بطاقة الائتمان على التفحص On line، وبعض المحافظ الالكترونية تحمل نقدا الكترونيا E.Cash وبعضها يحتوي على شهادات رقمية [26]. وأثناء التسوق في موقع فإنه يطلب معلومات موثقة للمستخدم، والمحفظة بإمكانها تقديم الشهادة تلقائيا.

المحور الثالث: الدفع الالكتروني بالبطاقة المغناطيسية وطرق وآليات الغش فيها

لم يعد مفهوم الدفع الالكتروني جديداً ، لأن عصر المعلوماتية ساهم في خلق عمليات جديدة تتناسب مع طبيعة الانتشار الواسع للشبكة العنكبوتية واستخداماتها. ومع انتشار جرائم الدفع الالكتروني توجب إيجاد قوانين حماية وتطبيقات آمنة لتسهيل عملية تحويل الأموال إضافة إلى أن الدفع الالكتروني يُعتبر عامل أساسي في تنمية وتطوير خدمات الحكومة الالكترونية والتجارة الالكترونية.

أولا- أشكال أنظمة الدفع الالكترونية: يتم الدفع الالكتروني في عمليات متصلة بشبكة إما عامة أو خاصة ، وعلى هذا الأساس فإن أنظمة الدفع الالكتروني تتم كأحد ثلاثة أشكال[27]:

1- الدفع عن طريق نقاط البيع Point of Sale: في حالة عدم توفر النقد الورقي حال الشراء فإنه يمكن للمشتري الدفع عن طريق البطاقة البنكية أو الائتمانية، تتم العملية عبر إمرار البطاقة على قارئ للشريط المغناطيسي الموجود خلف البطاقة، بعد ذلك يتم إدراج المبلغ المطلوب ثم يُطلب من المشتري إدخال الرقم السري. تُنقل معلومات الشراء عبر شبكة آمنة تماماً ويحصل المشتري على إيصال يتضمن أهم المعلومات عن هذه العملية للرجوع إليه عند الضرورة.

2- الدفع عن طريق أجهزة الصراف الآلي ATM's : الصرافات الآلية هي نظام معلومات متكامل يمكن عن طريقه السحب النقدي والقيام بعمليات مالية عديدة كالحوالات ونظام تسديد الفواتير أو المخالفات، وهي أيضاً تتم من خلال شبكة آمنة لمزامنة العمليات حتى لا تحصل حوادث سرقة أو اختلاس. إلى جانب العوامل الخارجية كتركيب كاميرات خاصة في أجهزة الصراف الآلي Pinhole Cam وكاميرات مراقبة في جميع مواقع الصرافات الآلية Surveillance Cam والتي تُزوَّد بأجهزة تسجيل تخزّن المواد المسجّلة لمدة لا تقل عن شهر كامل، يوجد أيضاً أجهزة تكشف محاولات الاحتيال Fraud Detection Device على جميع أجهزة الصراف الآلي.

3- الدفع عن طريق الشبكة العنكبوتية أو الانترنت World Wide Web: يختلف هذا الشكل من أشكال أنظمة الدفع الالكتروني في عدم اعتماده على أدوات محسوسة بشكل رئيسي كونها تعمل على الشبكة العالمية، وهو ما أوجب وضع بروتوكولات أمن وسلامة مثل بروتوكول SSL / TLS وهو ما سيتم التطرق إليه بالتفصيل.

ثانيا– وسائل الدفع عن طريق الانترنت: تتمثل في الآتي[28]:

1- النقد الرقمي Digital Cash: وهو أحد بدايات المدفوعات وهو ليس نقداً في الواقع ولكنه قيمة مخزنة ومن ثم متبادلة ولكن تحويلاتها محدودة لذلك نجح مثل هذا النوع في بيع الذهب لأنه أشبه بمبادلة النقد بالنقد.

2– الشيك الرقمي Digital Check: استخدامه نادر هدفه محاكاة الشيك التقليدي ولكن لأنظمة الدفع الالكتروني.

3- المحفظة الرقمية Digital Wallet: وظيفتها محاكاة مهام المحفظة التقليدية، فغالباً تحتوي على التالي:

أ – إثبات هوية مالكها ويتم ذلك باستخدام الشهادات الرقمية أو بخوارزميات تشفير أخرى.

ب– مكان لتخزين النقد ومبادلة القيمة النقدية.

ج – إدارة عمليات دفع آمنة من حساب المشتري إلى حساب متجر البائع.

4- نظام القيمة مسبقة الدفع الالكتروني: Online Stored Value Systems: يسمح هذا النظام للمستهلكين بالقيام بالعمليات الفورية وعمليات الدفع لحسابات المتاجر وحسابات الأفراد اعتماداً على قيمة مسبقة الدفع مخزنة في حساب المستهلك في البنك. ويعتبر PayPal النظام الأكثر نجاحاً في هذا المجال.

5- أنظمة دفع الحسابات التجميعية الرقمية Digital Accumulating Balance Payment System: تسمح للمستخدم بالقيام بالدفع للمبالغ الصغيرة والشراء عبر الانترنت وتجمع الحسابات ليتم فوترتها في نهاية كل شهر.

6- أنظمة الدفع اللاسلكية Wireless Payment System: تستعمل الأجهزة المحمولة الخلوية كجهاز للدفع. يتواجد مثل هذا النوع من أنظمة الدفع في بعض دول أوروبا وفي اليابان وكوريا الجنوبية. حتى الآن لم ينتشر بشكل واسع في الولايات المتحدة ولكن بدأت الأحوال تتغير مع دخول الشبكات اللاسلكية Wi-Fi وجوالات الجيل الثالث 3 G Cellular Phone.

ثالثا– طرق وآليات الغش في البطاقات الالكترونية: قد تُمارس بعض طرق الاستخدام غير المشروع لبطاقة الدفع الإلكتروني من أطراف البطاقة ذاتها وهي: الحامل، والتاجر، والمصدر، وقد يمارس بعضها الآخر من الغير، سواء في عمليات السحب من أجهزة الصرّاف الآلي أم في الوفاء، وسواء أتمّ الدفع للتاجر بواسطة البطاقة مباشرةً في وجود هذا الغير، أم من خلال شبكة الإنترنت. نذكر أهمها المتعارف عليها دوليا:

1– تزوير بطاقة الدفع الإلكتروني: الواقع أن تزوير بطاقة الدفع الإلكتروني أمرٌ صعب، إلا أنه ليس بمستحيل، وهو ما حدث فعلاً عندما قام أحد المهندسين بتقليد بطاقة وفاء، واستعملها كي يثبت أن وسائل الحماية للبطاقة غير كافية، كما أثبت أنه يمكن استخدام البطاقة المزوّرة في سحب الأموال من أجهزة الصرّاف الآلي باستخدام أرقام عشوائية بدلاً من الرقم السري للبطاقة [29].

يرد خبراء الكشف عن التزوير، طرق وأساليب تزوير بطاقة الدفع الإلكتروني ــ رغم تنوعها ــ إلى طائفتين هما:

أ– **التزوير الكلي:** إن خطوات التزوير الكلي لبطاقة الدفع الإلكتروني تتم بداية باصطناع البطاقة كاملةً، ثم تقليد الرسوم الخاصة على جسم البطاقة، وتغليفها، ولصق الهولجرام، والشريط الممغنط أو الشريحة الرقائقية، وشريط التوقيع، كل حسب موقعه الأصلي على جسم البطاقة، والقيام بالطباعة النافرة وتشغيلها عن طريق تغذيتها بالمعلومات التي حصل عليها المزورون من البطاقة الصحيحة.

ب– التزوير الجزئي: يستفيد المزور في هذه الحالة من جسم البطاقة الحقيقية، وما عليها من رسوم خاصة وحروف بارزة وكتابات أمنية، 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، يتمّ الحصول عليه بالطرق التي بيناها سابقا، أو تقليد الشريط الممغنط عن طريق محو ما عليه من بيانات وإعادة تشفيره بمعلومات جديدة صحيحة مسروقة، وقد يتمّ إجراء العمليتين معاً، كما يمكن أن يقوم المزور في هذه الحالة بكشط شريط التوقيع ووضع شريط آخر يتضمن توقيعه، أو يمحو آلياً أو كيميائياً التوقيع المثبت على الشريط ذاته ووضع توقيعه، كما يمكن أن يقوم المزور بخلع صورة حامل البطاقة الحقيقي، وتثبيت صورة شخص آخر مكانها.

1- طريقة السكيميغ: يتم التلاعب بأجهزة الصراف الآلي من قبل المجرمين لسرقة البيانات من الشرائط الممغنطة لبطاقات المصارف، والمعروفة بـ "سكيمينغ" أو الكشط Keystone، وفي معظم حالات كشط البطاقات المصرفية والائتمانية، يضع مُدبر عملية النهب داخل أجهزة الصراف الآلي أو في فتحة إدخال البطاقة جهازا يجمع البيانات المسجلة في الشريط

المغناطيسي للبطاقة المصرفية للضحية. ثم يحصل على الرقم السري، إما عن طريق كاميرا يتم تثبيتها فوق الصراف الآلي أو يحملها شخص يراقب صاحب البطاقة وهو يُدخل الرمز السري في الجهاز [30].

لأنه فور الحصول على هذين العنصرين الأساسين، أي البيانات الممغنطة والرقم السري، يتم نسخهما في بطاقة فارغة باستخدام جهاز ترميز [31]، ثم تُستخدم البطاقة الجديدة لشراء السلع وسحب المال.

2- الحصول على المعلومات السرية أو أسلوب التجسس Spying: حيث يقوم قراصنة الكمبيوتر باستخدام البرامج التي تتيح لهم الإطلاع على البيانات والمعلومات الخاصة بالشركات، والمؤسسات التجارية العاملة على شبكة الإنترنت، وبالتالي يتمّكنون من الحصول على ما يريدون من المعلومات، ومنها المتعلقة ببطاقات الوفاء التي استخدمت في التجارة الإلكترونية عبر الشبكة [32].

أ- القرصنة الالكترونية على حسابات البنوك: تعتبر القرصنة الالكترونية القائمة على الحسابات البنكية الالكترونية والمتمثلة بإرسال بريد الكتروني إلى العديد من العناوين الالكترونية لأشخاص لديهم حسابات في بنوك تقدم خدمات البنك الالكترونية عبر شبكة الانترنت يدعو صاحب الحساب البنكي إلى الدخول إلى رابط البنك المرفق مع البريد الالكتروني لإعادة إدخال اسم المستخدم وكلمة المرور نظراً لوجود تعارض في بياناته مع بيانات عميل أخر، وتكمن الخدعة في أن الرابط المرفق هو لموقع منسوخ طبق الأصل عن موقع البنك الذي يفترض أن لدى الضحية حساباً فيه وبمحاولة إتباع التعليمات وإدخاله لاسم المستخدم وكلمة المرور سيواجه الضحية بفشل محاولة استكمال العملية، وفي هذه الأثناء يكون المحتال قد نسخ هذه البيانات ليعود ويستخدمها لصالحه بتحويل الرصيد من حساب الضحية عبر الموقع الحقيقي للبنك بإدخاله للبيانات المسروقة.

ب- الاحتيال عبر الهواتف الخلوية: انتشرت مؤخراً استقبال الأجهزة الخلوية الخاصة بالعديد من المواطنين رسائل قصيرة (sms) محتواها أن صاحب الرقم قد فاز بمبلغ خيالي من خلال عبارات مختلفة للإيقاع بالضحايا وحيث أن الشركات الخلوية المختلفة لم تقم بإجراء مثل هذه المسابقات وتعتبر أسلوب احتيالي جديد من خلال سرقة معلومات الأشخاص الذين يقومون بالاتصال بالأرقام والعناوين المبينة في الرسائل القصيرة لغايات استخدامها في عمليات احتيالية الكترونية.

ج- تخليق أرقام البطاقة Card Math: وهو يعني تخليق أرقام بطاقة وفاء اعتماداً على إجراء معادلات رياضية وإحصائية، وهي كل ما يلزم للشراء عبر شبكة الإنترنت، فهذا الأسلوب يعتمد على أسس رياضية في تبديل وتوفيق لأرقام حسابية تؤدي في النهاية لناتج معين هو (الرقم السري) لبطاقة وفاء متداولة، ويتمّ استخدامها في معاملات غير مشروعة، عبر الشبكة، ومن هنا تأتي خطورة أن يكون كود البطاقة أو رقمها السري هو الضمان الوحيد لعدم اختراقها أو إساءة استعمالها[33].

3- البطاقة المسروقة أو المفقودة: وفي هذا النوع من الاستخدام نفرق بين الحالات التالية[34]:

أ_ سرقة البطاقة أو العثور عليها دون الرقم السري: وفي هذه الحالة، فإنّ الحائز للبطاقة المسروقة، أو المفقودة، لن يستطيع سحب الأموال من جهاز الصرّاف الآلي الذي سيقوم بسحب البطاقة عند الإدخال الخاطئ للرقم السري لثلاث مرات متتالية، أو سحب البطاقة من الجهاز حال الإبلاغ عن سرقة البطاقة أو فقدها من الحامل، وبرمجة البنك لأجهزة الصرّاف الآلي.

ب- **سرقة البطاقة أو العثور عليها مع رقمها السري:** وهي من أخطر الحالات، حيث يتمّكن الحائز للبطاقة المسروقة، أو المفقودة مع علمه برقمها السري من سحب الأموال من جهاز الموزع الألي للاوراق النقدية ضمن الحد الأقصى المسموح به للسحب اليومي، وذلك قبل إبلاغ الحامل للبنك المصدر عن سرقة البطاقة، أو فقدها.

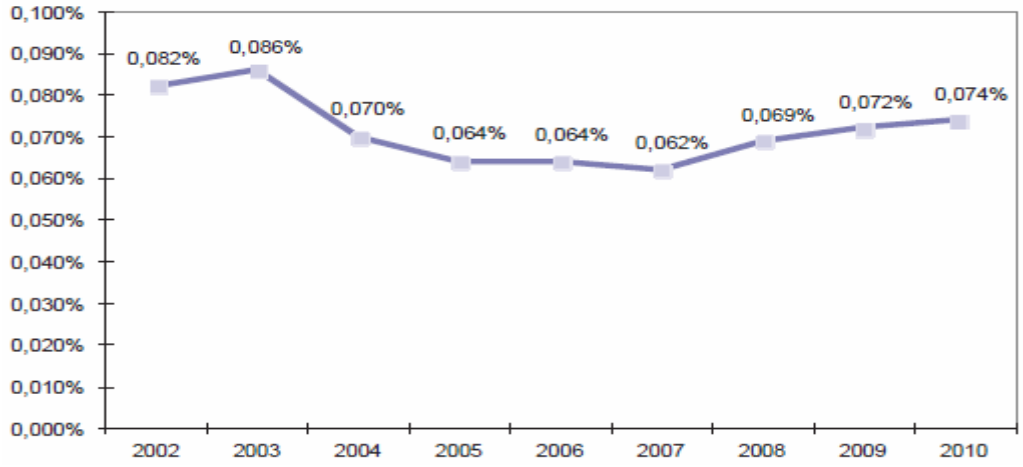
ج- استخدام البطاقة المسروقة أو المفقودة في الوفاء: عند قيام الغير بسرقة البطاقة، أو العثور عليها بعد فقدها، فإنّه يتجه عادة إلى استخدامها فوراً، مستغلاً بذلك الفترة التي تقع بين تاريخ تقديم البلاغ إلى الجهة المصدرة وبين تاريخ قيام هذه الأخيرة بإلغاء التعامل بالبطاقة، أو التعميم عليها من خلال الأجهزة الإلكترونية (P.O.S) الموجودة لدى التجار المربوطة بالأجهزة الإلكترونية للمُصدر، أو قبل توزيع القوائم التي تحمل أرقام البطاقات الملغاة، كما أنّ هذا الغير الحائز للبطاقة المسروقة أو المفقودة يفضل التعامل بها مع التجار الذين يستخدمون الأجهزة اليدوية؛ لان الحماية للبطاقة في هذه الحالة تكون أقل بكثير من الحماية الممنوحة للبطاقة من خلال الأجهزة الإلكترونية.(P.O.S) .

المحور الرابع: طرق الغش والجرائم المختلفة باستخدام البطاقة الالكترونية في فرنسا

تؤكد جميع المؤشرات أن الجرائم الإلكترونية مرشحة للارتفاع، إذا لم تبادر السلطات المختصة إلى اتخاذ التدابير الضرورية لمواجهة هذا المشكل والتصدي للخطر المحدق بالاقتصاد الوطني نحاول من خلال هذا المحور معرفة هذه الظاهرة وتتبع حيثياتها في البلدان المتقدمة كمثال على ذلك أخذنا فرنسا [35]. ما يميز قطاع النقديات فيها أنه عرف نموا مطردا في السنوات الأخيرة، ويظهر من خلال ارتفاع عدد الشبابيك الأوتوماتيكية وحاملي البطاقات البنكية.

أولا- معدلات الغش بخصوص كل أنواع البطاقات: مع توسع استعمال هذه الوسائل الجديدة في المعاملات التجارية والاقتصادية خصوصا، حيث تعتبر فرنسا من أكثر الدول المتضررة بالجرائم الالكترونية، حيث يرتفع فيها معدلات الغش بخصوص استخدام البطاقات بصفة عامة سنويا.

الشكل رقم (02) معدل الغش في جميع أنواع البطاقات في فرنسا



Source: **L'Observatoire de la sécurité des cartes de paiement**, huitième rapport d'activité concernant l'année 2010.P.22, **http://www.banque-france.fr/observatoire/home.htm**

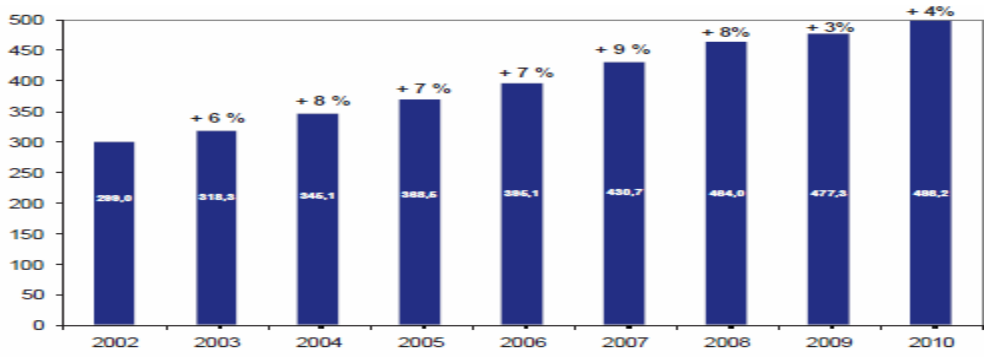
نلاحظ من خلال الشكل أعلاه أن معدل الغش المتعلق ببطاقات السحب والدفع المسجلة في عام 2010 في فرنسا بلغ 0.074٪، وهو معدل مرتفع مقارنة مع دول مماثلة، بارتفاع طفيف مقارنة مع السنوات السابقة 2009 و 2008، وانخفض متوسط مبلغ الصفقة الاحتيالية الى 122 اورور مقابل 136 سنة 2009 [36].

وأن هذا االارتفاع كانت بداياته سنة 2007 بعدما كان في انخفاض مستمر ابتداء من سنة 2003 أين عرفت هذه الاخيرة أعلى معدل للغش بلغ 0.086٪، في العشر سنوات الأخيرة.

ثانيا–العلاقة بين حجم الصفقات والتعاملات ومعدلات الغش في البطاقات:

1– حجم الصفقات في الاقتصاد الفرنسي: إن الشكل الموالي يوضح حجم الصفقات والمعاملات بصفة عامة في الاقتصاد الفرنسي ابتداء من سنة 2002 إلى غاية سنة 2010.

الشكل رقم(03): حجم الصفقات في فرنسا(بالمليار اورو)

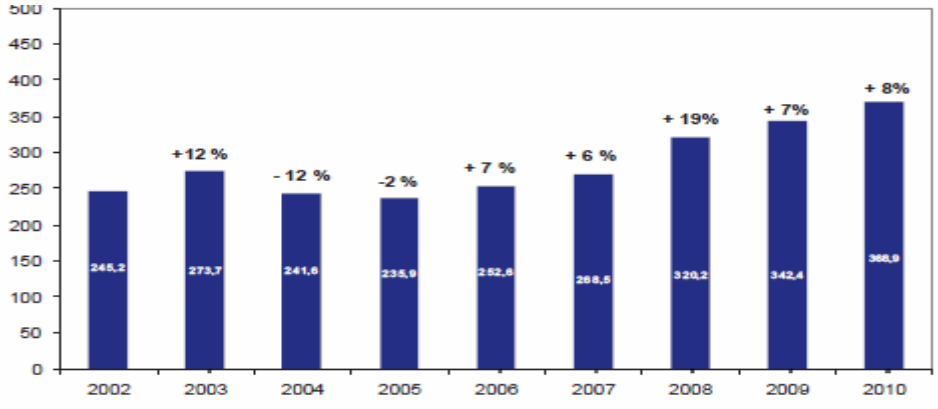


Source: **L'Observatoire de la sécurité des cartes de paiement,** huitième rapport d'activité concernant l'année 2010.P.22, **http://www.banque-france.fr/observatoire/home.htm**

يوضح الشكل أن حجم الصفقات في فرنسا في ارتفاع مستمر من سنة 2002 إلى غاية سنة 2010 أين وصلت 488 مليار أورو بعدما كانت 477 مليار أورو، سنة 2009 أي بمعدل ارتفاع 4% وبفارق يقدر 11 مليار أورو، حيث أن أكبر نسبة ارتفاع كانت سنة 2007 بمعدل 9% .

2- الغش والتزوير الخاص بكل أنواع بطاقات الدفع: والشكل التالي يوضح الغش الخاص بكل أنواع البطاقات.

الشكل رقم(04) تطور حجم مبالغ الغش والتزوير إجمالا في فرنسا



Source: L'Observatoire de la sécurité des cartes de paiement, huitième rapport d'activité concernant l'année 2010.P.22, **http://www.banque-france.fr/observatoire/home.html**

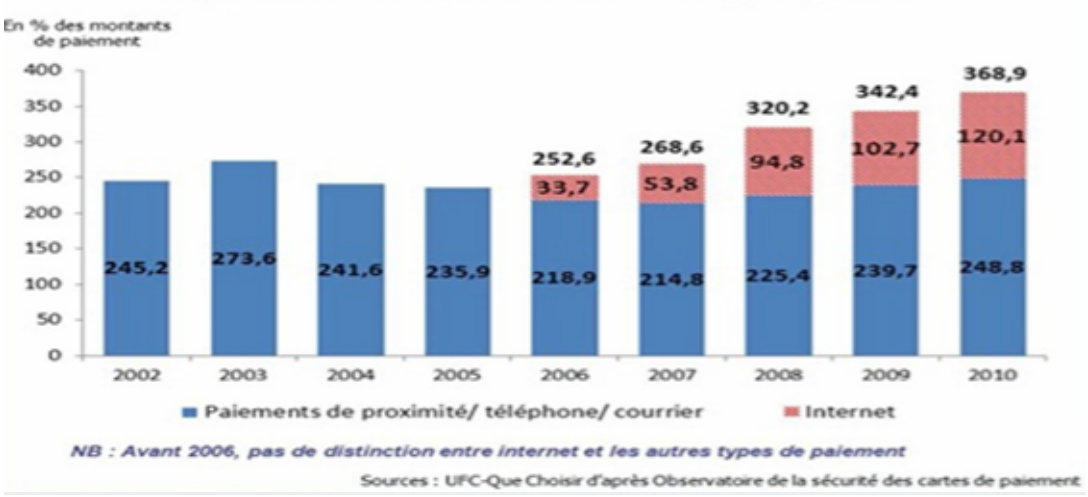
نلاحظ من خلال الشكل أن حجم المبالغ المغشوشة والمزورة في ارتفاع مستمر منذ 2005، أين كان حجم المبالغ 235 مليون أورو ليصل سنة 2010 **إلى** 368 مليون أورو أي بمعدل ارتفاع قدره 8% عن سنة 2009 أين وصل حجم الغش 342 مليون اورو، وأكبر حجم ارتفاع في مبالغ الغش كان سنة 2008 وقدر بـ 320 مليون اورو بعدما كان سنة 2007 يقدر بـ 268 مليون أورو. أي بمعدل ارتفاع قدرة 19%.

نستنتج في الأخير أنه كلما ارتفعت حجم الصفقات في الاقتصاد الفرنسي ارتفعت معدلات الغش في البطاقات، وبالتالي هناك علاقة طردية بين الصفقات ومعدلات العش في البطاقات، خاصة وأن المعاملات في الاقتصاد الفرنسي تتوجه إلى النمط الالكتروني شيئا فشيئا.

ثالثا: تطور خسائر عمليات الغش حسب طريقة الدفع:

1- تطور حجم مبالغ الغش والتزوير حسب طريقة الدفع: بغية توضيح تطور مبالغ الغش استعنا بالشكل الموالي.

الشكل رقم(05): تطور حجم مبالغ الغش والتزوير حسب طريقة الدفع



Source : **La rédaction de ZDNet.fr** ZDNet France. Publié le vendredi 17 février 2012 ;**http://www.zdnet.fr/actualites/le-cout-de-la-fraude-bancaire-sur-internet-ne-conna-t-pas-la-crise-39768686.htm**

إن تطور التجارة الإلكترونية أدى أيضا إلى تفاقم ظاهرة تزوير بطاقات الائتمان على الإنترنت حيث في عام 2010 كلف هذا التزوير نحو 120 مليون يورو وفقا لـ UFC [37] والتي اتهمت جمعية المصارف ومراكز البيع الإلكترونية الفرنسية بعدم القيام بأي شيء. وأنها غير راضية عن مكافحة التزوير والتحايل لبطاقات الائتمان عبر الإنترنت.

- **الملاحظة الأولى:** التزوير والاحتيال على الإنترنت ينمو باستمرار، حيث وصلت إلى 0.276٪ من المدفوعات المحلية

و 1.36٪ من المدفوعات الدولية في عام 2010 وهو أكبر من المعدل العام للتزوير الدفع الذي بلغ 0.074 ٪

الملاحظة الثانية: ليس وحده التزوير في ارتفاع فقط ، بل وتعتبر أيضا مكلفة، فحسب الجمعية فإن شبكة الإنترنت تمثل 5٪ من المعاملات، حيث أن 33٪ من المبلغ الإجمالي للتزوير المصرفي، أي ما يقابل 120.1 مليون اورو سنة 2010، فمن 62.6٪ من حالات التزوير تتمثل في سرقة معلومات بطاقة الائتمان عند الدفع، فعلى سبيل المثال تتأسف UFC على بعض المواقع "لا يوجد أي التزام لإبلاغ الزبائن عند وجود فيروس، مما جعل من الصعب وضع التدابير اللازمة، وبسبب تزايد عدد البطاقات المصرفية في التداول (29٪ بين عامي 2002 و 2010)، وتطور التجارة الإلكترونية والدفع عبر الإنترنت، أدى ذلك إلى نمو ظاهر التزوير والغش في حين يتحمل في نهاية المطاف تكلفة الاحتيال من قبل المستهلك، الآمر الذي أدى بـ UFC. وجمعية المستهلك بالعمل على نصائح أهمها اعتماد نظام لحماية دفع موحدة، مثل تأمين D3.

2- معدلات الغش في البطاقات في المعاملات المحلية: إن نمط الدفع بواسطة البطاقة التي اعتمدها مرصد L'Observatoire مختلف من نمط إلى نمط آخر، حيث ميز بين المدفوعات بالقرب من الأجهزة sur automate في نقاط البيع Point de Vente أو موزعات الوقود، تذاكر النقل...، والمدفوعات عن بعد (عبر الإنترنت، البريد، والهاتف، الفاكس... الخ) والسحب.

لقراءة أفضل، فإن التطورات في أعقاب البيانات المحلية الفرنسية موضحة أسفل الجدول.

الجدول رقم(01):معدل الغش بالبطاقات حسب نمط العملية(سحب أو دفع)

Transactions nationales	2006	2007	2008	2009	2010
Paiements	**0,035 % (92,3)**	**0,032 % (95,6)**	**0,036 % (111,7)**	**0,038 % (123,2)**	**0,041 % (137,3)**
- dont paiements de proximité et sur automate	0,024 % (59,1)	0,017 % (45,4)	0,015 % (44,5)	0,014 % (41,0)	0,012 % (36,2)
- dont paiements à distance	0,199 % (33,2)	0,236 % (50,1)	0,252 % (67,2)	0,263 % (82,2)	0,262 % (101,1)
- dont par courrier / téléphone	0,194 % (19,8)	0,201 % (23,8)	0,280 % (28,5)	0,263 % (30,3)	0,231 % (27,3)
- dont sur Internet	0,208 % (13,4)	0,281 % (26,4)	0,235 % (38,8)	0,263 % (51,9)	0,276% (73,9)
Retraits	**0,019 % (17,4)**	**0,020 % (19,0)**	**0,018 % (19,1)**	**0,019 % (20,8)**	**0,024 % (26,5)**
Total	**0,031 % (109,6)**	**0,029 % (114,5)**	**0,031 % (130,9)**	**0,033 % (144,0)**	**0,036 % (163,8)**

Source: L'Observatoire de la sécurité des cartes de paiement, huitième rapport d'activité concernant l'année 2010.P.25, **http://www.banque-france.fr/observatoire/home.htm**

من خلال الجدول نلاحظ أن معدل الغش في عمليات الدفع المحلية بلغ 41% سنة 2010 وحجم المبالغ المغشوشة كان 137,3 مليون أورو، وهذا الارتفاع كان ابتداءا من سنة 2007 أين وصلت حجم المبالغ المغشوشة 95,6 مليون أورو.

ما يلاحظ أن الغش في عمليات الدفع بالقرب من الأجهزة يتخفض من سنة الى أخرى أي من سنة 2006 أين بلغ معدل الغش 24 % ليصل المعدل 12 % سنة 2010، ولكن على العكس تماما بالنسبة لعمليات الدفع عن بعد (البريد، الهاتف، الإنترنت) أين نجد أن معلات الغش في تزايد مستمر ابتداء من سنة 2006 حيث كان حجم المبالغ المغشوشة 33,2 مليون أورو لتصل سنة 2010 إلى 101,1 مليون أورو.

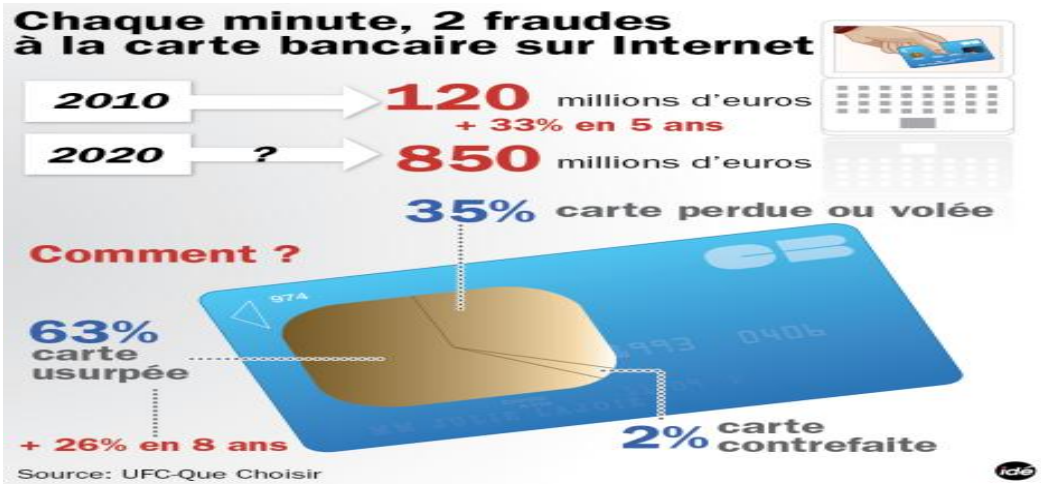
أما بخصوص عمليات السحب فقدرت حجم الخسائر بـ 26,5 مليون أورو بعدما ارتفعت سنة 2010 مقارنة بسنة 2009 و2008و 2007 و2006 ، وما يلاحظ كذالك هو الارتفاع التدريجي لمعدلات الغش في 5 سنوات الأخيرة.

رابعا- البطاقات البنكية المزورة على الانترنت وكيفية الوقاية في فرنسا:

1- عملية الغش في البطاقة البنكية على شبكة الانترنت: يوضح الشكل أسفله أن في كل دقيقة هناك عملية غش في البطاقة البنكية على شبكة الإنترنت، وقدر حجم الخسارة بـ 120 مليون أورو سنة 2010 كما توضيحه من خلال الشكل رقم(**05**) أي بمعدل 3% في مدة 5 سنوات. ويتوقع أن تصل حجم الخسائر إلى 850 مليون أورو سنة 2020، أما بخصوص عمليات الغش التي مست البطاقة البنكية فتوردها كما يلي:

- 35 % من البطاقات مسروقة أو ضائعة.
- 63 % من البطاقات تم السطو عليها.
- 2 % من البطاقات مزورة أو مزيفة.

الشكل رقم (06): توضيحات بخصوص الغش بالبطاقات البنكية على شبكة الانترنت



Source : Chaque minute, deux fraudes à la carte bancaire sur Internet ; Créé le 16/02/2012 à 20h52 **http://www.rtl.fr/actualites/internet/article/chaque-minute-deux-fraudes-a-la-carte-bancaire-sur-internet-7743854435**

2- خدمات ثلاثية الأبعاد الآمنة لحاملي بطاقات الائتمان 3D : هذا النظام موجود بالفعل ولكن أعتمده 13٪ فقط من التجار على الانترنت. فلماذا أكثر أمنا؟ لأنها تزود المشتري بكلمة مرور لا يعرفها سواه، بحيث لا يعرفها البائع ولا يكون مسؤولا عن التقاطها وهو ما سَيُسَاعِد على تقليل المخاطر من خلال طريقتين [38]:

_ نسخ تفاصيل البطاقة، إما عن طريق كتابة الأرقام على البطاقة نفسها، أو عن طريق نهايات معدلة أو أجهزة الصراف الآلي، ولا ينتجُ عن ذلك القدرة على الشراء عبر الإنترنت بسبب كلمة المرور الإضافية، والتي لا يتم تخزينها أو كتابتها على البطاقة.

إن عدم التقاط التاجر لكلمة المرور، يقلِلُ من مخاطر حدوث الحوادث الأمنية في التجارة عبر الإنترنت، بينما قد لا يزال الخطر قائما من احتمال حصول القراصنة على التفاصيل الأخرى للبطاقة، حيث أنه في هذه الحالة لا توجد لهم وسيلة في الحصول على كلمة المرور المرتبطة بها.

وانخفض الاحتيال والتزوير بنسبة 50٪ في 4 سنوات في المملكة المتحدة التي تستخدم هذا النظام ويستخدم هذا الرمز او النظام 3D من قبل 96% من تجار التجزئة _التجار على الخط أو على الانترنت **Commerçants en ligne** في

المملكة المتحدة، كما انخفض الغش بـ 50% في 4 سنوات، إلا أنه لا يستخدم هذا النظام في فرنسا على نطاق واسع من الاستخدام لعدة أسباب أهمها ما يلي:

- عدم وجود تنسيق حقيقي بين البنوك ومراكز البيع الإلكترونية.
- كل بنك له نظام تحديد الهوية الخاص به مما يعقد عملية التنفيذ.

وطالب الاتحاد الفدرالي لجمعية حماية المستهلك البنوك الاعتماد على نظام لتحديد الهوية بواسطة نظام 3D الآمن، وهذا بعد أن تعتمده جميع مراكز البيع الإلكترونية.

المحور الخامس: كيفية الوقاية من الظاهرة تزوير البطاقات الالكترونية

أولا– تجميد البطاقة: يلاحظ اليوم أيضا زيادة كبيرة في عدد البطاقات التي تم تجميد استخدامها من قبل المؤسسات المصرفية والمالية بسبب شكها في وجود نشاطات مشبوهة [39]، ويتم ايقاف استخدام عدد من البطاقات كإجراء احترازي للوقاية من عمليات الاحتيال.

ثانيا– تغيير الرقم السري: الشيء الذي يقام به بصورة أكثر انتظاما، لا أعتقد أن هنالك الكثير مما يمكن القيام به. الشيء المثير للقلق بهذا الشأن هو أن المجرمين يبدون مُتقدمين بخطوة على البنوك. ويستدرك قائلا: "من الواضح أنك تحتاج إلى الحد الأدنى من التجهيزات لترميز البطاقة، ولم تكن تلك الأجهزة متاحة على الإطلاق قبل بضع سنوات، بحيث كان استخدامها مقتصرا على المهنيين. أما اليوم، فقد أضحت مُنتشرة وبات بالإمكان اقتناؤها من خلال ملء طلبية على الإنترنت بسعر غير مكلف على الإطلاق.

ثالثا– تحذيرات بشأن عملية السحب من الموزعات: تقدم البنوك والمؤسسات المالية العالمية على غرار الفرنسية مجموعة من الارشادات والتعليمات للعملاء بشأن عمليات السحب:

- القيام بتغطية اليد التي يُدخل بها الرقم السري باليد الأخرى لكي يمنع تصويره من أية زاوية.
- أو القيام بكتابة الرقم السري بسرعة قصوى مستخدما اليدين في نفس الوقت.
- التأكد من عدم وجود أي شخص يراقب العميل أثناء إدخال الرمز السري.
- إذا لوحظ أنه تم العبث بجهاز الموزع أو الشباك الآلي أو فتحة الجهاز التي تسمح بقراءة محتويات البطاقة، يجب إبلاغ السلطات المختصة.
- بعد استخدام البطاقة، لا بد من التأكد من وضعها على الفور في مكان آمن.
- إذا ظلت البطاقة عالقة في الجهاز، يجب الاتصال على الفور بالبنك أو المؤسسة المالية لكي يجمد استخدامها.
- اجتناب استخدام أجهزة الموزعات الألية للاوراق النقدية في الليل.

رابعا– بروتوكول الحماية SSL / TLS: تستخدم البنوك والمؤسسات المالية بروتوكولات الحماية، ففي الاتصالات الآمنة والأكثر شيوعاً تستخدم بروتوكولي SSL/TLS وهما Secure Sockets Layer and Transport Layer Syecurit ، فبروتوكول SSL طوّر من قبل شركة Netscape لنقل المستندات بطريقة آمنة عبر الانترنت. هذا البروتوكول يستخدم مفتاح خاص لتشفير المعلومات المتبادلة على اتصال. SSL ما يتم الآن استخدامه في الاتصالات هو النسخة الثانية من البروتوكول.يوجد بروتوكول آخر هو Personal Communication Technology ويرمز له بالرمز PCT وهو شبيه جداً ببروتوكول SSL إلا أنه يستخدم خوارزميات أكثر تقدماً ومفاتيح تشفير أطول وهو من تطوير شركة مايكروسوفت Microsoftأعقب ذلك صدور بروتوكول TLS ويعتبر إضافة على بروتوكول SSL ويسمّون معاً SSL / TLS ليضمن الخصوصيPrivacy ودقة البيانات Data Integrity بين كل تطبيقين متصلين عن طريق الانترنت.بشكل عام يتكون بروتوكول SSL/TLS من طبقتين[40]:

أ- **بروتوكول مصافحة الأيدي** TLS Handshake Protocol: ويستخدم لإثبات شرعية الخادم server والتابع client والتفاوض في خوارزمية التشفير ومفاتيحه قبل السماح للبيانات بالانتقال بين الخادم والتابع.

ب- **بروتوكول التسجيل** TLS Record Protocol: ويسمح للخادم والتابع بالاتصال فيما بينهما باستخدام نماذج خوارزميات التشفير أو بدون تشفير عند الحاجة لذلك. إن أكثر الاستخدامات شيوعاً في الاتصالات الآمنة بين الخادم والتابع تستخدم بروتوكول SSL وهي عبارة عن http بسيط محمول على SSL/TLS ويتميز نطاق المواقع التي تستخدمه بابتدائه بـ https:// وظهور رمز قفل في نافذة المتصفح.

المحور السادس: تزوير بطاقات السحب البريدية والبنكية الجزائرية[41]:

البنوك والمؤسسات المالية الجزائرية مازالت بعيدة كل البعد عن واقع استخدام الدفع الالكتروني كما هو متعامل به في الدولة المتقدمة عامة وفرنسا خاصة، حيث تقتصر البطاقات البريدية والبنكية الجزيرية على عمليات السحب فقط من الموزعات النقدية للأوراق النقدية أو الموزعات الالية البنكية المتواجد في الأماكن العمومية وعلى جدران البنوك ومراكز البريد، لكن ما راج مؤخرا في المجلات والجرائد الوطنية أن مصالح الأمن الحزائرية المختصة في مكافحة الجريمة الاقتصادية، تسعى حاليا تحقيقات معمقة حول تداول بطاقات مغناطيسية مزورة، لسحب الأموال عبر مختلف الموزعات الآلية، حيث تقوم شبكات مجهولة بترويجها بعد سرقة الأرقام السرية من أصحاب البطاقات من أجل استخدامها وسحب أموال المواطنين من أرصدتهم.

_ التحقيق الذي شرعت فيه مصالح الأمن جاء بناء على معلومات تفيد بتداول بطاقات مغناطيسية مزوّرة خاصة بسحب الأموال في العاصمة وبالضبط في باش جراح، القبة، وسط الجزائر، بئر مراد رايس وغيرها من بلديات العاصمة وامتد بيعها إلى الولايات المجاورة على غرار بومرداس، تيبازة، والبليدة، تقوم بترويجها مجموعة من الأشخاص احترفوا التزوير

في البطاقات الرمادية، حسب المعلومات المتوفرة لدى مصالح الأمن، التي تتحرى حاليا في الكشف عن ملابسات هذه الجريمة التي تهدد بشكل من الأشكال، حسابات المواطنين، وفي هذا السياق، طمأن وزير البريد وتكنولوجيات الإعلام والاتصال موسى بن حمادي، في تصريح لـ "الشروق" للمواطنين، مؤكدا أن التزوير في البطاقات المغناطيسية واردا، لكن استعمالها في سحب الأموال من الموزعات الآلية مستحيل، إذا لم يتحصل أصحابها على الأرقام السرية وكلمات العبور من أصحابها الحقيقيين.

وأوضح بن حمادي أن الموزعات الآلية مزود بنظام خاص يقوم بحجز البطاقة بصفة أوتوماتيكية في حال تسجيل الرقم السري بطريقة خاطئة للمرة الثالثة، وإعادتها يتطلب الرجوع إلى القابض بشروط محدودة، وهذا كإجراء احترازي لحماية صاحب البطاقة الحقيقي، في حين دعا ذات المتحدث، أصحاب البطاقات المغناطيسية إلى ضرورة توخي الحيطة في حالة إدخال أرقامهم السرية الخاصة بهم لسحب أموالهم وتوخي الحذر من سرقتها من طرف شبكات إجرامية تستعملها لغرض الاستيلاء على أرصدة المواطنين.

وأضاف المسؤول الأول عن قطاع البريد، أن تزوير البطاقات المغناطيسية في الدول الغربية، يتم بإستعمال البطاقات الحقيقية، التي عادة ما يتم الاستحواذ عليها بطرق مختلفة من أصحابها الشرعيين واستعمالها باللجوء إلى برامج معلوماتية عالية الدقة لقراءة، وكشف الأرقام السرية وكلمات العبور، وهي الأمور التي تعتبر محدودة جدا في الجزائر بسبب تواضع استعمال بطاقات الدفع بالجزائر التي لا تستعمل حاليا بها في الغالب سوى بطاقات السحب.

الخاتمة:

تشير الاحصائيات إلى ارتفاع عدد أعمال القرصنة عالميا في سوق بطاقات الائتمان، وكما تم التأكيد عليه من خلال هذه الدراسة التي شملت فرنسا كواحدة من الدول المتقدمة في مجال أليات الدفع الالكتروني، وبالتالي يمكن القول أن فرنسا تعاني من عمليات التزوير في البطاقات بصفة عامة، وهذا نتيجة لانتشار استخدام الشبكة العنكبوتية (الإنترنت) خلال السنوات القليلة الماضية، وأيضاً تطور أدوات القرصنة المعلوماتية القادرة على اختراق جدران الحماية والأجهزة المخصصة لحماية الشبكة والأدوات والوسائل التقنية المشغلة لها.

حيث لوحظ في فرنسا أنه كلما ارتفع حجم الصفقات والمعاملات التجارية ارتفع معدل الغش بالبطاقات في الاقتصاد الفرنسي.وهي تعمل جاهدة على الحد من هذه الظاهرة الاجرامية.

تصنف عمليات القرصنة المعلوماتية دوليا ضمن الجريمة المنظمة والتي تخضع لتنظيم محكم في أغلب الأحيان من قبل جماعات تعتمد أحدث الوسائل بطرق خبيثة. وقد تفطنت العديد من المؤسسات المالية لهذه الممارسات واتخذت إجراءات لتأمين عمليات إذ اعتمدت بعض البنوك نظام المراقبة العالمية تحت اسم Close monitoring بالاستعانة ببرمجيات حديثة تسمح بمحاربة السرقات البنكية.

إذن يمكن القول في الأخير أن عمليات التدليس من خلال البطاقات الالكترونية بصفة عامة لا تشمل الدول المتقدمة فحسب وإنما كذلك المتخلفة والسائرة في طريق النمو كالجزائر بالرغم من طرق الوقاية الحديثة.

التوصيات: في الأخير ومن أجل القضاء على جرائم الغش والتزوير في بطاقات السحب البريدية والبنكية ارتأينا تقديم التوصيات والاقتراحات التالية مستفيدين من التجربة الفرنسية:

– العمل على حماية المواطن والعميل الجزائري من هذه الممارسات الإجرامية وغير القانونية والشرعية من خلال إصدار بطاقات بنكية وبريدية تخضع إلى مواصفات عالمية من حيث سلامة العمليات المالية كبطاقة VISA وCard Master .

– العمل على وضع نظام مراقبة خاص بالموزعات الآلية للأوراق النقدية الخاصة بالبنوك أو مراكز البريد ذا علاقة مباشرة بالحاسوب المركزي للموزعات، وبإمكان هذا النظام الكشف عن أغلب عمليات التحايل التي يمكن أن تقع.

– أهمية تبادل الخبرات والمعلومات مع عنصر أساسي في إنجاح التعاون في مجال مكافحة هذه الجرائم ومواجهة هذا التحدي الدولي.

– المتابعة والتنسيق المستمر مع الجهات والسلطات المختصة ذات الصلة محليا ودولياً فيما يتعلق بعمليات تزوير بطاقات السحب والدفع الالكتروني.

– مراجعة القواعد القائمة حاليا لمكافحة هذه الجرائم من أجل تطوير هذه القواعد وتحسينها وتوجه القضاة ورجال الشرطة والدرك الوطني إلى التخصص في مجال الجرائم المالية.

– إنشاء وحدة خاصة في الشرطة القضائية لمكافحة الجريمة المالية والجريمة الالكترونية، والتجربة الفرنسية خير دليل على ذلك.

– إنشاء مكاتب مكافحة الجرائم المالية وتبييض الأموال كما هو الحال في فرنسا مع تدريب عناصر قوى الأمن الداخلي ومضاعفة يقظة كل المصالح بنوك، شرطة، الجمارك، الدرك الوطني، وإنشاء قاعدة بيانات بخصوص ممارسات التحايل وعمليات التزيير، والبطاقات المسروقة والمجمدة...

– طمأنة وزير البريد وتكنولوجيات الإعلام والاتصال موسى بن حمادي لايكف، بل يجب العمل على تطوير أجهزة مكافحة التزوير والتحايل.

– تدعيم مبدأ تبادل المعلومات بين المسؤولين الماليين في القطاع البنكي والمالي بالتنسيق مع شركة SATIM والجمعية للبنوك والمؤسسات المالية ووزارة الداخلية وشركة "فيزا" العالمية.

– العمل على تأكيد الاتفاق على إنشاء لجنة إفريقية لمكافحة التحايل بالبطاقة البنكية. وسيكون أعضاء هذه اللجنة رؤساء اللجان الوطنية لمكافحة التحايل بالبطاقة البنكية في كل بلد مشارك

– ضرورة إطلاق البنوك والمؤسسات المالية الجزائرية حملات للتعريف بأنواع عمليات الاحتيال والنصب المالي والمصرفي، وخاصة المتعلقة باستخدام البطاقة البينكية la Carte CIB، التي يمكن أن يتعرض لها عملاء البنوك والبريد في حالة عدم اتباعهم للتعليمات والإرشادات والتحذيرات التي تصدرها باستمرار، بما في ذلك الأضرار التي من الممكن أن تلحق بهم.

المراجع والهوامش:

[1] عطا الله خليل، مدخل مقترح لمكافحة الفساد في الوطن العربي، ورقة عمل مقدمة في ندوة المال العام ومكافحة الفساد الإداري والمالي، المنظمة العربية للتنمية الادارية، تونس،14-18 ماي2007، ص. 11.

[2] الفساد المالي والإداري...إرهاب مقنع، http://arabic.rt.com/forum/archive/index.php/t-4374.html

[3] عصام البشير، الفساد المالي وأثره على الفرد والمجتمع، http://www.fikercenter.com/fiker/index.php?option=com

[4] محمود كبيش، السياسة الجنائية في مواجهة غسيل الأموال، دار النهضة العربية، ط2 ، بند 1، 2001، ص. 8.

[5] دليل عمل نشاط الإدارة العامة لمباحث الأموال العامة، مطبوعات وزارة الداخلية المصرية، يناير 1999، ص. 193.

[6] عبد محمود هلال السميرات، عمليات غسيل الأموال بين الاقتصاد الوضعي والاقتصاد الإسلامي، مذكرة مقدمة كجزء من متطلبات الحصول على شهادة ماجستير في الاقتصاد والمصارف الإسلامية، قسم الاقتصاد والمصارف الإسلامية، جامعة اليرموك، عمان، الأردن، 1998،ص.21.

[7] رافعة إبراهيم الحمداني، أثر استخدام التكنولوجيا المصرفية في ظاهر غسيل الأموال والجهود الدولية لمكافحتها، المؤتمر العلمي الرابع حول استراتيجيات الاعمال في مواجهه تحديات العولمة،جامعة فيلاديلفيا ، يومي14-15،2005، ص.9.

[8] بابكر الشيخ، غسيل الاموال، _أليات المجتمع في التصدي لظاهرة غسيل الأموال_، مكتبة الحمل للنشر والتوزيع، عمان، الأردن، 2003، ص.37.

[9] فتحي شوكات مصطفى عرفات، بطاقات الائتمان البنكية في الفقه الاسلامي، مذكرة مقدمة استكمالا لنيل درجة الماجستير في الفقه والتشريع، كلية الدراسات العليا بجامعة النجاح الوطنية بنابلس، فلسطين، 2007، ص. 7.

[10] سميحة القليوبي، وسائل الدفع الحديثة، أعمال المؤتمر العلمي السنوي لكلية الحقوق بجامعة بيروت العربية _ أعمال المصارف من الوجهتين القانونية والاقتصادية_، منشورات الحلبي الحقوقية، بيروت، لبنان، 2002، ص. 67.

[11] يوسف أحمد أبو فارة، التسويق الالكتروني _عناصر المزيج التسويقي عبر الانترنت_، دار وائل للنشر ، عمان، الأردن، 2004، ص. 375_376.

[12] طارق عبد العال حماد، التجارة الالكترونية، الدار الجامعية، القاهرة، ج م ع، 2003، ص. 128.

[13] عبد الهادي النجار، بطاقات الائتمان والعمليات المصرفية الالكترونية، أعمال المؤتمر العلمي السنوي لكلية الحقوق بجامعة بيروت العربية – أعمال المصارف من الوجهتين القانونية والاقتصادية–، منشورات الحلبي الحقوقية، بيروت، لبنان، 2002، ص.37-38.

[14] سميحة القليوبي، مرجع سابق، ص. 67.

[15] المرجع السابق، ص. 67.

[16] pre-paid and/or stored value cards

[17] منير وممدوح محمد الجنبيهي، البنوك الالكترونية، دار الفكر الجامعي، الاسكندرية، ج م ع، 2005 ص. 50-51.

[18] يطلق عليها بالفرنسية La Carte à Puce

[19] يوسف أحمد أبو فارة، مرجع سابق، ص. 376-377.

[20] طارق عبد العال حماد، مرجع سابق، ص. 123.

[21] للاطلاع على كيفية الانتقال من بطاقات الائتمان التقليدية إلى البطاقات الذكية، أنظر:

- Michel Badoc et Autres, Marketing de la Banque et de l'Assurance, Edition d'Organisation, Paris, France, 2ème Edition, 2000, P. 58-61.

[22] المحفظة الالكترونية Electronic Wallet http://www.alexalaw.com/t6947-topic

[23] الموسوعة العالمية ويكيبيديا، http://ar.wikipedia.org

[24] يطلق عليها بالفرنسية La Porte Monnaie Electronique

[25] منير وممدوح محمد الجنبيهي، مرجع سابق، ص. 53.

[26] طارق عبد العال حماد، مرجع سابق، ص. 117.

[27] روان عبدالرحمن العبدان، تطبيقات آمنة في عمليات الدفع الالكتروني، المقالات العلمية، مركز التميز لأمن المعلومات، ص. 5. أنظر الموقع الالكتروني التالي: http://coeia.edu.sa/images/stories/PDFs/Applications_in_secure_electronic_payment.pdf

[28] روان عبدالرحمن العبدان، مرجع سابق، ص. 5.

[29] امجد حمدان الجهني، استخدامات غير المشروعة لبطاقات الدفع الإلكتروني من قبل الغير، وزارة العدل– المجلس القضائي، المملكة الأردنية الهاشمية، ص. 15. http://www.cojss.com/replay.php?a=174

[30] صوفي دووي، لدى سحب المال ببطاقاتك المصرفية والإئتمانية... حذاري من السّرقة المنظمة، 21 جويلية 2011، مقال منشور على شبكة الانترنت، انظر الموقع الالكتروني التالي: http://m.swissinfo.ch/ara/detail/content.html?mobileTopicId=29730894&view=mobileDetail&cid=30465004

[31] إن استخدام تكنولوجيا الشريط المغناطيسي أصبحت أكثر شيوعا في السنوات الأخيرة في إطار تطبيقات أخرى غير الخدمات المصرفية، لاسيما في ظل توافر أجهزة الترميز وسهولة اقتنائها على الإنترنت.

[32] من الأمثلة من سحب من رصيد أحد عملاء البنوك الحكومية عن طريق شبكة الإنترنت، واستخدما هذه المبالغ في مشاهدة أفلام متنوعة على الإنترنت، وتبين أنهما استطاعا معرفة الرقم السري لحساب العميل على هذه الشبكة عن طريق التجسس واستغلاه في مشاهدة هذه الأفلام على مدى شهور.

[33] امجد حمدان الجهني، مرجع سابق، ص. 11.

[34] المرجع السابق، ص. 12.

[35] تكشف الإحصاءات التي أجراها مُوفر الخدمات المصرفية في سويسرا SIX Group بأن عدد أجهزة الصراف الآلي في سويسرا التي تعرضت لعمليات التلاعب من قبل المجرمين بهدف كشط البطاقات المصرفية والائتمانية قد ارتفع إلى 32 آلة في عام 2009، ثم إلى 135 في 2010، قبل أن يقفز إلى 225 آلة خلال الأشهر الأربعة الأولى من هذا العام. http://m.swissinfo.ch/ara/detail/content.html?mobileTopicId=29730894&view=mobileDetail&cid=30465004

[36] L'Observatoire de la sécurité des cartes de paiement, OP,Cit, P,22,

[37] L'Union Fédérale des Consommateurs—Que choisir ou UFC—Que choisir est une association par André Romieu. Elle a pour objectif de défendre les intérêts des consommateurs. 1951créée en http://fr.wikipedia.org/wiki/Union_F%C3%A9d%C3%A9rale_des_Consommateurs_-_Que_Choisir

[38] أخبار عرب نت، مصرف السلام والمصرف البحريني السعودي شريكان لشركة الخدمات المالية العربية، أخبار واراء اقتصادية، http://www.akhbaralarab.net/index.php/financial/47582-2012-02-19-09-06-39

[39] فمثلا في سويسرا ارتفع عدد البطاقات المجمدة من 6200 في عام 2009 إلى قرابة 22000 في الأشهر الأربعة الأولى من عام 2011.

http://www.akhbaralarab.net/index.php/financial/47582-2012-02-19-09-06-39

[40] روان عبدالرحمن العبدان، مرجع سابق، ص, 4.

[41] نوارة بشوش، بطاقات مغناطيسية مزورة لسحب الأموال من البنوك والبريد، الموقع الالكتروني لجريدة الشروق، جريدة وطنية يومية جزائرية، 4 جانفي 2012. http://www.echoroukonline.com/ara/index.php?news=89842