

«LAWYER»

الإطار القانوني للدفع الإلكتروني

ان بروز عمليات البيع والخدمات عبر شبكة الإنترنت، طرحت بشكل اساسي الإشكاليات المتصلة بوسائل الدفع الإلكترونية. ان اغلبية عمليات الدفع الإلكتروني على شبكة الإنترنت تقع على مبالغ مالية صغيرة وهي تتطلب أماناً معيناً ضرورياً، على السواء بالنسبة للمستهلك والبائع، سيما وان الدفع يؤدي الى تنفيذ او انقضاء الموجب القانوني. يوجد اليوم العديد من الوسائل المقترحة للدفع الإلكتروني، مما يطرح اشكالية مدى تألف الخدمات المصرفية مع الخدمات الغير مصرفية للدفع عبر الشبكة

Charbel Kareh
PhD – Attorney At Law

www.charbelkareh.com

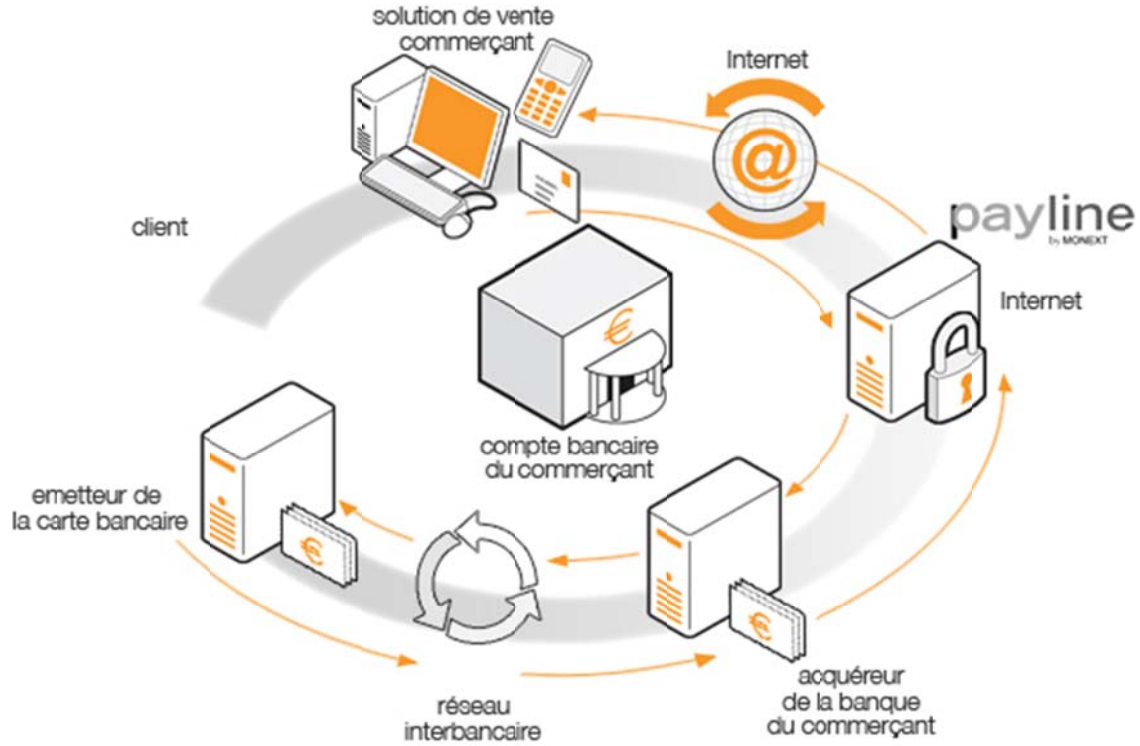


أولاً: الإطار التعاقدى مع المصارف وأنواع الدفع الإلكتروني

ان وضع اية وسيلة دفع الكتروني آمن وذات مصدقية عبر الشبكة، يتطلب بشكل عام واساسي تدخلاً مصرفياً. فالتاجر الإلكتروني الذي يودّ تفعيل آلية الدفع الإلكتروني على موقعه، يكون مجبراً على توقيع عقدان مع المصرف: الأول يسمى عقد بيع عن بعد (" Vente A Distance" : Contrat de VAD) والثاني عقد محطة دفع الكتروني. (" Terminal de Paiement Electronique" : Contrat de TPE) .

في عقد البيع عن بعد، يكون على التاجر التقدّم من مصرفه بطلب تعاقد، محددًا نسبة العمولة المصرفية على المبيعات عبر الشبكة، ليصار الى تزويده برقم تاجر ورقم آلة، التي تسمح له بتفعيل خدمة الدفع الإلكتروني. ان ابرام هذا العقد يبقى خاضعاً لتقييم المصرف، وفقاً لمعايير تكون متصلة بأقدمية الحساب المصرفي ونوعية العميل، إضافة الى طبيعة البضائع والخدمات المراد تسويقها عبر الشبكة.

اما بالنسبة لعقد انشاء محطة الدفع الإلكتروني، فهو عقد مرن، ليس بالضروري ابرامه مع مصرف التاجر الإلكتروني مباشرة، اذ من المستحسن اللجوء الى مؤسسات مالية او شبه مصرفية متخصصة بعمليات الدفع الرقمي والتحويل وادارة حسابات الكترونية، سيما لكونها متخصصة ومتألّفة مع عقود البيع عن بعد الخاصة بالمصارف.



آلية الدفع الإلكتروني عبر الشبكة¹

يوجد اليوم عدة أنواع للدفع الإلكتروني، نذكر أبرزها: البطاقة المصرفية العادية، محفظة النقود الإلكترونية، الدفع عبر البريد الإلكتروني (Paypal)، الدفع عبر الشيك الإلكتروني أو الدفع عن بعد (Télépaiement). تشكل البطاقة المصرفية أولى وسائل الدفع الإلكتروني وتسمى بالدفع عبر ادخال ١٦ رقماً، وهي البطاقة الكلاسيكية التي تحوي على ١٦ رقماً ظاهراً على البطاقة مع اسم معين وتاريخ صلاحية ورقم ثلاثي للمصادقة، والتي يصار الى ادخالها في كل مرة يريد فيها الفرد الشراء عبر الشبكة.

¹ - http://www.google.com.lb/imgres?imgurl=http://www.orange-business.com/fr/entreprise/portfolio/catalogue/toutes-solutions/att00011434/87164_236919.jpg&imgrefurl=http://www.orange-business.com/fr/entreprise/services-solutions/relation-client/paiement-sans-contact/payline/&usg=__buNBom7GOLZ_56v3xMZyZV2dVhc=&h=385&w=580&sz=86&hl=ar&start=5&zoom=1&tbnid=DXci4rsfSkTfzM:&tbnh=89&tbnw=134&ei=Eb_IT5v3JcHj4QTP2O21AQ&um=1&itbs=1



البطاقة المصرفية ذات الرأس الذكي^٢

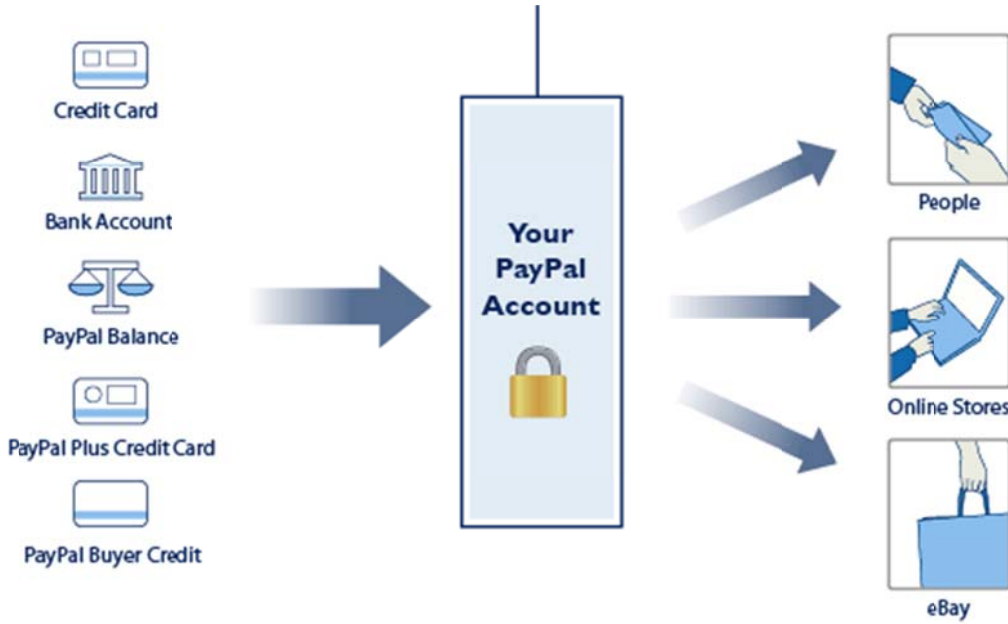
وتصدياً للأنظمة التي تعمل عبر تقنيات مضادة للتشفير، والتي تسمح بالإستعلام عن رقم البطاقة، قامت اليوم العديد من المصارف بتطوير بروتوكولات خاصة بالدفع الآمن عبر الشبكة والتي تحجب بيانات البطاقة وتمنع انتقالها عبر الشبكة الرقمية كبروتوكول العمليات الإلكترونية الآمنة “Secure Electronic Transaction” de Visa et Mastercard) اما محفظة النقود الإلكترونية^٣ فهي عبارة عن بديل إلكتروني للنقود تخزن على سند إلكتروني سواء على رأس ذكي للبطاقة المصرفية او على ذاكرة الحاسوب الآلي، وهذه النقود الإلكترونية تكون مدفوعة مسبقاً وسلفاً وبقيم صغيرة، تهدف الى إجراء عمليات

² - http://www.google.com.lb/imgres?imgurl=http://www.prepaidvirtualcreditcards.com/visa-classic-credit-card.jpg&imgrefurl=http://www.prepaidvirtualcreditcards.com/&usq=__hRddJ_nWydBf_m_hCK_urEDKR_U=&h=311&w=484&sz=31&hl=ar&start=1&zoom=1&tbnid=3iYaktz0QilbaM:&tbnh=83&tbnw=129&ei=h77IT47WIeiM4gTQtpzGAQ&um=1&itbs=1

³ - لدراسة معمقة، راجع النقود الإلكترونية، شريل القارح وغسان الخوري، دراسة تحت اشراف الرئيس الدكتور جوزف سماحه، دراسات عليا في المعلوماتية القانونية، جامعة الحكمة، ٢٠٠١.

دفع إلكتروني من حساب معيّن مدفوع سلفاً للمصرف ومحدد القيمة.

اما الدفع عبر البريد الإلكتروني او ال Paypal ، فهو عبارة عن شركة تسمح لمستعملي الشبكة بفتح حسابات لديها عبر موقعها الإلكتروني وتعبئة هذا الحساب بنقود الكترونية، ومن ثم تخوّل المستهلك الدفع عبر تحديد البريد الإلكتروني للتاجر الإلكتروني. بعد تحديد البريد الإلكتروني والقيمة المتوجبة، يستلم التاجر بريداً إلكترونياً يحوي على وصلة نص فائق تحيله الى موقع Paypal الآمن الذي يسمح له بقبض الثمن.



كيفية تعبئة حساب Paypal⁴

My Account Send Money Request Money Merchant Tools Auction Tools

Pay Anyone Pay for eBay items

Send Money [Secure Transaction](#)

You can pay anyone with an email address in the 55 countries and regions that accept PayPal.

Recipient's Email:

- OR - Select a recipient

Amount:

Currency: U.S. Dollars

Category of Purchase: - Please Select Type -

Email Subject (optional)

Note (optional)

آلية الدفع عبر البريد الإلكتروني أو ال PayPal °

بالنسبة للشيك الإلكتروني، تقوم بعض المواقع المالية بتزويد الأشخاص بدفتر شيكات إلكتروني يمكن للمستعمل رؤيته، فتحه وتعبئه ويحرك انطلاقاً من حساب إلكتروني يعبأ سلفاً مثل نظام eCheck⁵ du أما الدفع عن بعد فيتضمن أنظمة مختلفة تستعمل التقنيات المعلوماتية والخطوط الهاتفية بغية تسهيل عمليات الدفع بين فرقاء متباعدين سواء عبر وسطاء ماليين أو من دونهم.

⁵ - http://www.google.com.lb/imgres?imgurl=http://www.hotscams.com/content_images/paypal-0207-2.jpg&imgrefurl=http://www.hotscams.com/articles/warning-another-paypal-phishing-scam.html&usg=__SFJap7AnETuwXo5u9sK-hjC6_Rc=&h=569&w=663&sz=84&hl=ar&start=96&zoom=1&tbnid=mqi1fOQPYP2WpvM:&tbnh=118&tbnw=138&ei=NMTT4b6H8TT4Qsf8_jJAQ&um=1&itbs=1

⁶ - eCheck: <http://www.echeck.org>.

Prénom Nom 059
 Adresse
 Ville, USA, code postal

Montant payable à _____ \$ _____

 DOLLARS

Votre Banque

Nom _____

059 67354 007 0525-00054

Numéro de série du chèque Code de transit de l'agence à 5 chiffres ID de l'institution à 3 chiffres Numéro de compte

الشيك الإلكتروني^٧

ثانياً: عناصر الدفع الإلكتروني

يتميز الدفع الإلكتروني بعدة خصائص تتناسب وطبيعة الشبكة. أولاً: العالمية التي تسمح بالدفع عبر الشبكة لدى كافة المواقع على المستوى العالمي. ثانياً: بالدفعات الصغيرة وبسرعة تنفيذ العملية المالية مما يقلص من الخسائر في حال حصول غش أو احتيال. ثالثاً: سهولة الإستعمال اذ يكفي ادخال بضعة بيانات ليصار الى انهاء العملية المالية، اما الأهم فهو التأكد من مصداقية النقود الإلكترونية. في الواقع، تتميز هذه الأخيرة بكونها عبارة عن بيانات رقمية، ومثل اي بيانات معلوماتية الكترونية يمكن ان تتعدد نسخها الى ما لا نهاية، اذ من المستحيل التمييز بين الأصل والنسخة الإلكترونيين. لذلك يجب اللجوء الى انظمة دفع إلكتروني تمنع

الصرف المزدوج للنقود الإلكترونية (Double-Spending). ويفضل الأنظمة المصرفية المتصلة عبر الشبكة بشكل آني، لم يعد هذا الأمر مطروحاً. ويبقى ان نشير الى ضرورة احترام الدفع الإلكتروني لعناصر امان العملية المالية، التأكد من هوية الفراء والسرية.

ان ابرز ما يخشاه اليوم المستهلك الإلكتروني عند اقدمه على الدفع عبر الشبكة، هو عملية التسليم ونوعية التاجر الإلكتروني، اضافة الى حماية بياناته الشخصية. فالدفع الإلكتروني يتطلب ادخال بيانات بطاقات الدفع عبر نماذج مخصصة لذلك في الموقع الإلكتروني، وهي البيانات التي تمكّن من تنفيذ العملية المالية وبالتالي تحويل المبلغ المطلوب الى حساب التاجر الإلكتروني. اضافة الى البيانات الإسمية لكل بطاقة دفع تستعمل عبر الإنترنت، لا بد من الإشارة الى ضمانات المستهلك الإلكتروني في مرحلة ما بعد تنفيذ العملية المالية عن بعد. ونتكلم هنا عن النظام الحمائي للمستهلك والذي يتعلق مباشرة بالتسليم خلال مهل محددة او الغاء البيع واسترداد الثمن في حال تم البيع بواسطة البطاقات المصرفية، اضافة الى حق اعادة البضاعة المشتراة ضمن شروط معيّنة. لذلك، يكون على المستهلك واجب التنبه والتعاقد فقط مع المؤسسات ذات المصادقية والجديّة عبر الشبكة، او تلك التي تحمل مصادقات معيّنة او اختام ثقة والتي تضمن احترام تعهدات التاجر الإلكتروني.

في الواقع، ان امان عمليات الدفع الإلكتروني يرتكز على مصادقة اطراف العملية، على صحة وسرية البيانات المتبادلة، على نهائية الدفع الإلكتروني وعلى اشفة العملية الإلكترونية. فيما يتعلق بمصادقة اطراف العملية، فهي تُنَبَّت، عبر أنظمة التوقيع الإلكتروني، حصول الدفع وتسمح للمشتري بالتأكد من حقيقة وجود التاجر الإلكتروني، وبالمقابل تعطي التاجر الإلكتروني ضمانات الشخص الثالث المصادق وبالتالي الثقة في

هوية المستهلك التي طلب الشراء عبر موقعه الإلكتروني. ان البيانات المرسله عبر الشبكة تتطلب احترام معياري الصحة والسرية ايضاً، وهي تتلخص بالبيانات المصرفية للمستهلكين (رقم بطاقة، تاريخ صلاحية، تشفير بصري، اسم حامل البطاقة...) والتي يجب ان لا تتغير اثناء انتقالها عبر الشبكة مع وجوب بقائها سرية. ويبقى ان يكون الدفع، متى تم عبر الإنترنت، نهائياً لا يمكن الرجوع عنه من قبل المشتري باستثناء بعض الشروط القانونية المحصورة. واخيراً لا بد من حفظ تاريخ العمليات بأرشفة آمنة وصادقاً بغية تقديم الدليل والإثبات على عمليات الدفع الإلكتروني في أي وقت يحصل فيه اعتراض او نزاع حولها. ان الدفع الإلكتروني هو عادة نهائياً لا يمكن الرجوع عنه، لكن في حالات قانونية محددة، يمكن للمستهلك ان يعترض لدى مصرفه ويطلب استرجاع الثمن. ويتم ذلك في حال (١) تم الدفع نتيجة احتيال او غشّ معينين عن بعد ومن دون استعمال مادي للبطاقة، او في حال (٢) تم تزوير البطاقة، وكانت بطاقة المستهلك في حيازته لحظة تنفيذ عملية الدفع الإلكتروني عن بعد.

ثالثاً: مخاطر الدفع الإلكتروني

على المستوى القانوني، ان اية وسيلة دفع الكتروني تتطلب اولاً تحديد هوية عاطي أمر الدفع، وثانياً مصادقة الجهة المالية على هذا الأمر، تمهيداً لتنفيذه. ويتم ذلك عبر ادخال الرقم السري الذي يربط بين رقم التعريف والبطاقة، وهو شكل من اشكال التعبير عن رضی صاحب البطاقة الإلكترونية الذي يسمح بتنفيذ العملية المالية. اما الأهم في هذه العملية، فهو نظام التشفير المستعمل الذي يشكل الضمانة لسرية المعلومات

المتناقلة عبر الشبكة^٨.

في فرنسا مثلاً، يكون لكل شخص وقع ضحية استعمال غير مشروع لبطاقة المصرفية ٩٠ يوماً للإعلان وإبطال عمليات الغش، اما في الولايات المتحدة الأمريكية، فإن هذه المهلة هي محددة ب ٣٠ يوماً مع حصر مسؤولية المستهلك ب ٥٠ دولاراً اميركياً^٩. لكن في هذه الحالات، يخشى التاجر عدم دفع قيمة البضائع او الخدمات المباعة، مما يشكّل عائقاً امام التجارة الإلكترونية. لذا يكون على التاجر الإلكتروني واجب أخذ بعض إجراءات الأمان بغية الحدّ من مخاطر الغش لأي استعمال للبطاقة المصرفية عبر موقعه. اما مهلة الاعتراض نتيجة فقدان او سرقة بطاقة الدفع في فرنسا، فهي محددة ب ٤٨ ساعة مع احتمال تحميل صاحب البطاقة السحوبات المسحوبة قبل تقديمه لإعتراضه لغاية سقف محدد.

وفي دعوى عرضت على محكمة التمييز الفرنسية، قام المصرف بتحميل صاحب البطاقة مبلغاً وقدره ٢٧٤٣/ يورو سحب قبل الاعتراض بحجة انه تم سحب المبلغ عبر استعمال الرمز السري للبطاقة مما يثبت اهمال صاحب البطاقة في الحفاظ على الرقم السري. وقررت بالتالي الغرفة التجارية لمحكمة التمييز الفرنسية في قرار حديث لها انه يقع على المصرف مُصدّر البطاقة عبء اثبات ان صاحب البطاقة قد اخطأ او اهمل في حماية رقم بطاقته السري، وان مجرد استعمال البطاقة من قبل شخص ثالث ليس كافياً لإقامة الدليل^{١٠}.

⁸ - Pour une étude exhaustive, Charbel Karez, L'argent électronique, Mythe ou réalité? Mémoire d'un DEA en Informatique Juridique, Sous la direction du Président Joseph Samaha, Université La Sagesse, 2002.

⁹ - Pierre Paul LEMYRE, Chapitre 8, Le paiement électronique, Disponible à partir du site: http://www.jurisint.org/pub/05/fr/guide_chap8.pdf, P. 150.

¹⁰ - Arrêt de la Cour de cassation du 2 octobre 2007, n° 05-19.899, La Poste c/ Marie-Claude X, Disponible à partie du site: <http://www.juriscom.net/actu/visu.php?ID=969>.

في الواقع، على كل تاجر الكتروني التقيّد بالإجراءات التالية لضمان تنفيذ عمليات الدفع الإلكتروني: (١) التأكد من موافقة مؤسسة الدفع، (٢) التأكد من رمز او عنوان المصادقة (AVN: Address Verification Service)، ففي حال كان جواب المؤسسة المالية سلبياً: التواصل مع المؤسسة المالية بغية الحصول على مصادقة مستعمل البطاقة ومصرفه، واذا كان الجواب ايجابياً: التأكد من عنوان تسليم البضاعة، التأكد من نوعية وكمية البضاعة المراد تسليمها، التأكد من طريقة التسليم، والتأكد من صحة البريد الإلكتروني^{١١}.

ان التوقعات المستقبلية على المدى المنظور تذهب باتجاه توحيد لأنظمة الدفع على الشبكة. ولكون التجارة بحدّ ذاتها تتميز بطبيعتها الدولية، فإن اعتماد وسيلة دفع عالمية من قبل التجار تتطلب قبولاً من قبل المستهلك والمؤسسات المالية، وبدأنا نشهد اليوم تراجعاً من قبل اللاعبين الأساسيين على حساب المؤسسات الكبرى التي تعمل على تنمية وتقوية الإقتصاد الليبرالي على الشبكة.

ونشير ختاماً بشكل وجيز الى ان الساحة المصرفية تشهد خلال العشرية الأخيرة توسعاً كبيراً في التكنولوجيا المصرفية ولو بتفاوت بين المؤسسات المصرفية، حيث يتم إجراء عمليات مصرفية بشكل إلكتروني على شبكة الإنترنت او غيرها من الشبكات المغلقة، كتقديم خدمات السحب والدفع والتحويل دون انتقال العميل إليها. وتبرز اهمية المصارف الإلكترونية، في تقديم خدمات مصرفية كاملة وجديدة، خفض التكاليف وزيادة كفاءة المصارف الالكترونية، اضافة الى خدمات البطاقات على انواعها. لكن في المقابل، تواجه المصارف الالكترونية مخاطر عدّة ابرزها: (١) المخاطر التقنية التي تتمثل في احتمال الخسارة أو حصول أخطاء من

¹¹ - Pierre paul LEMYRE, Ibidem, P. 151.

قبل العملاء، أو في برنامج إلكتروني غير ملائم أو يفقد إلى الامان والتشفير الضروريين، (٢) مخاطر الاحتيال وتتمثل في تقليد البرامج أو تزوير معلومات مطابقة للبرامج الالكترونية، (٣) مخاطر ناتجة عن سوء عمل النظام الالكتروني، (٤) مخاطر قانونية تحدث عندما لا يحترم المصرف القواعد القانونية والتشريعات المنصوص عليها سيما في حال غياب تشريعات خاصة بالمعاملات الإلكترونية والتوقيع الإلكتروني، (٥) مخاطر فجائية قد تؤدي إلى مشاكل في السيولة وفي سياسة القروض المصرفية، (٦) وأخيراً مخاطر تكنولوجية ترتبط بالتغيرات التكنولوجية السريعة.