

LETTRE D'INFORMATION : **BON A SAVOIR** (N°25)

**Une société promet des virements internationaux
sans frais bancaires**

Un cauchemar pour les banques? Une société estonienne lancée par des concepteurs de Skype et Paypal réinvente les transferts d'argent en mettant en relation des personnes ayant des besoins de change complémentaires. Frontaliers, ne pas s'abstenir

Vous en avez assez de payer des frais bancaires sur vos virements internationaux? TransferWise, un nouvel outil internet lancé par deux Estoniens passionnés de hightech, permet d'effectuer ce type d'opérations sans passer par les banques.

«Adieu les banques, vous avez fait votre temps!», raille le site internet fondé par Taavet Hinrikus et Kristo Kaarmann, 31 et 32 ans, spécialistes des systèmes d'appels internet gratuits Skype et de paiement en ligne Paypal.

TransferWise, lancé en janvier 2011 et dont l'utilisation est facturée 1 livre sterling (1,2 euro) pour tout transfert d'argent jusqu'à 230 euros (0,5% au delà), a déjà généré 60 millions d'euros de chiffre d'affaires et la croissance est de 20% par mois, assurent-ils.

Les virements internationaux suscitent des frais bancaires compris généralement entre 3% et 6%, avec des taux de change arrondis en faveur des opérateurs.

TransferWise a des clients dans toute l'Europe et plus particulièrement en Grande-Bretagne, en France et en Espagne, selon ses dirigeants.

Hinrikus était le directeur de la stratégie de Skype jusqu'en 2008. Kaarmann était consultant pour les cabinets d'audit Deloitte et PricewaterhouseCoopers avant de lancer TransferWise.

L'idée leur est venue alors que Hinrikus vivait à Londres et réglait ses dépenses en livres mais était payé en euros par Skype, société basée dans son Estonie natale. Kaarmann de son côté était payé en livres à Londres mais il remboursait sa maison en euros à Tallinn.

«Nous avons constaté que nous avions des besoins de change complémentaires et nous avons commencé à changer de l'argent entre nous au taux médian du marché -- le taux que vous trouvez dans les journaux, pas le taux majoré que vous propose votre banque», dit Hinrikus à l'AFP.

«On s'est rapidement rendu compte qu'on économisait une fortune en évitant les virements internationaux et on s'est dit que ce serait peut-être une bonne idée commerciale. C'est ainsi que TransferWise est né», ajoute-t-il.

Une idée toute simple

Le système consiste à relier des gens ayant des besoins de change complémentaires.

Ainsi, un client en Grande-Bretagne qui veut envoyer de l'argent chez lui en Estonie peut mettre des livres sur un compte TransferWise, explique Hinrikus. La société recherche alors un client en Estonie qui a besoin de faire la même opération en sens inverse et l'invite à déposer ses euros sur TransferWise, ajoute-t-il.

Au lieu d'envoyer l'argent d'un pays à l'autre, TransferWise verse à chaque client le montant demandé converti en livre ou en euro au taux de change médian du marché à un coût très réduit.

Mais le système ne pourrait-il pas être détourné pour blanchir de l'argent?

Donata Huggins, porte-parole de TransferWise, assure que ce service a reçu l'approbation de la Financial Services Authority (FSA), l'organisme chargé de la réglementation de l'industrie des services financiers au Royaume-Uni.

Ce qui signifie qu'il est soumis aux mêmes règles commerciales que les banques au Royaume-Uni. «Les fonds de nos clients sont placés sur des comptes séparés des comptes bancaires d'affaires», précise-t-elle.

TransferWise emploie 25 salariés et a reçu environ 1 million d'euros d'investissements provenant de différentes sources, comme le fondateur de Paypal, Max Levchin et l'homme d'affaires français Xavier Niel, co-actionnaire du quotidien Le Monde et patron de Free.

Liens : <http://www.letemps.ch/no-section/2013/02/16/une-societe-promet-virements-internationaux-frais-bancaires>

En finir avec les banques dans 10 ans ?

Aujourd'hui, grâce à la révolution numérique, chacune des fonctions qu'une banque remplit actuellement peut être faite plus vite, de façon plus efficace et sans intermédiaire central en utilisant les technologies numériques.

Le transfert d'argent n'a de nos jours plus besoin d'un établissement bancaire centralisé. Des applications comme Abra ou, pour les échanges monétaires en devises, Transferwise permettent de répondre à des problématiques complexes de façon élégante, simple et décentralisée, en concurrence. Et les banques ne pourront pas fournir un service équivalent sans changer profondément de métier.

Les habituels services de gestion de compte sont, eux aussi, appelés à évoluer bien au-delà des « home-bankings » proposés par les banques historiques. Mint en est un exemple assez flagrant qui propose de rassembler en un point unique tous les comptes et toutes les opérations bancaires pour les présenter de façon efficace sur différents supports. Dans la même veine, chacune des start-ups présentées dans cet article de Capital illustre une façon de se passer de la banque traditionnelle ou d'en contourner les services.

Mais plus important encore, les cryptomonnaies, Bitcoin en tête, représentent la révolution fondamentale qui donnent toutes les briques de base nécessaires à la remise en question complète du concept même de banque. Bitcoin, déjà évoqué de nombreuses fois dans ces colonnes, se passe de tout point centralisateur tel que le serait une banque. En outre, là où tout échange monétaire nécessite actuellement un tiers de confiance (joué par le système bancaire dans l'écrasante majorité des cas), Bitcoin propose un système fonctionnant sans tiers de confiance : les transactions sont infalsifiables, non répudiables, et définitives.

On peut arguer de la grande volatilité des cours de Bitcoin pour ne voir dans cette innovation technologique qu'un gadget amusant et voué à l'échec, mais la réalité est que cette cryptomonnaie est une excellente preuve de concept par l'exemple : oui, une cryptomonnaie peut fonctionner sans tiers de confiance ni système bancaire, oui, des transactions commerciales peuvent être menées en l'utilisant, et oui, le marché peut arriver, seul, à déterminer la valeur et la pérennité de cette monnaie sans l'intervention d'un *Deus Ex Machina* ou d'une banque centrale politisée. On comprend que ces caractéristiques rendent particulièrement moites les mains de banquiers, de politiciens ou même de syndicalistes.

Et très concrètement, Bitcoin aura permis l'émergence d'un bouillonnement de projets dans le domaine, visant à répondre à différentes problématiques monétaires et bancaires. Outre des variantes plus ou moins sérieuses de cryptomonnaies, on trouve différentes initiatives de regroupement de briques technologiques (cryptomonnaie, système de paiements, plate-forme

de trading, ...) comme par exemple SuperNet, plate-forme d'échange en pair-à-pair (sans centralisation, donc).

Comme on le voit, on assiste au développement de plus en plus rapide d'organisations autonomes fortement distribuées, qui se passent très bien de toute permission d'un État pour effectuer les transactions, et qu'empêcher, réguler ou encadrer s'avérera impossible (ou trop coûteux), par la nature même de ces innovations. En outre, les voitures à chevaux n'ont pas évolué avec des chevaux plus rapides. Les abaques ne sont pas devenus électriques. Les banques telles qu'on les connaît n'évolueront pas en réseaux décentralisés, elles seront remplacées.

Et si les révolutions précédentes (depuis les appareils photos numériques jusqu'aux biotechnologies en passant par l'impression 3D) sont un indicateur du rythme auquel on doit s'attendre, il est probable qu'il ne faudra pas vingt ans pour un tel changement. Or, d'après un récent rapport de ... Goldman Sachs (une banque, eh oui), dans les sondés de la Génération Y (qui ont la trentaine actuellement), 33% admettent s'attendre à pouvoir se passer complètement d'une banque dans les cinq à dix ans à venir, et 50% estiment que l'une ou l'autre start-up aura, d'ici là, pris le relais de ces dernières...

Lorsqu'on voit ce que les hommes d'État ont fait du système bancaire actuel, lorsqu'on voit à quel point ils ont corrodé l'idée même de monnaie et de comportements économiques sains, on comprend que déposséder l'État du système bancaire et renvoyer celle-ci vers les citoyens est **un objectif à la fois noble et nécessaire**.

Et, maintenant que la technologie le permet, c'est même atteignable.

Liens : <http://www.contrepoints.org/2015/05/08/207050-en-finir-avec-les-banques-dans-10-ans>

Les banques organisent la riposte face aux fintech, dans les transferts d'argent

C'est maintenant qu'il faut agir. » Tel est, en substance, le message que les banques membres de Swift (Society for worldwide interbank financial telecommunication) avaient adressé à ce réseau mondial d'échange de données financières, en 2015, lors du salon Sibos organisé par ce dernier. L'objet de cette urgence ? La modernisation des infrastructures de paiements internationaux de Swift. Il faut dire que la création de cette coopérative belge - qui compte quelque 10.000 adhérents dans 200 pays environ, dont 7.000 banques - remonte aux années 1970. Certes, Swift - qui permet aux banques d'échanger des informations financières automatisées et standardisées, donc à moindre coût - représente toujours « *une grande partie des paiements internationaux interbancaires, entre pays nécessitant une conversion de devises, qu'il s'agisse de paiements au bénéfice d'entreprises ou de particuliers* », a souligné Thierry Chilos, l'un des responsables de Swift pour la zone Europe, Moyen-Orient, Afrique, lors d'une conférence de presse, le 11 mars.

Mais cette position devient plus difficile à tenir, depuis quelques années. D'abord parce que les nouvelles technologies ont considérablement modifié les attentes des utilisateurs finaux de Swift. Désormais habitués à voir nombre de leurs demandes satisfaites quasi-instantanément, d'un simple glissement du pouce sur l'écran de leur smartphone, ils ne comprennent plus qu'envoyer de l'argent à l'étranger prenne deux à cinq jours, quand ce n'est pas dix jours pour certains pays. Une durée qui n'est qu'agaçante pour la clientèle des particuliers, mais qui devient carrément problématique dans le domaine du commerce international. En 2016, il n'est en effet pas simple pour un fournisseur d'admettre que son paiement par le donneur d'ordre mette plus de temps à franchir les mers que les navires chargés d'acheminer sa cargaison.

L'émergence de nouveaux acteurs

Si, encore, il n'y avait que le problème du délai des transferts d'argent internationaux. Mais non. Particuliers comme entreprises, les utilisateurs finaux de Swift réclament également un service meilleur marché, davantage de transparence sur les tarifs afin de savoir exactement quelle somme le bénéficiaire recevra, ainsi qu'une plus grande traçabilité des transactions, entre leur déclenchement et le moment où le compte du bénéficiaire est crédité, un peu à la manière de que proposent DHL et UPS dans le transport de colis. Ces nouvelles exigences, Swift doit les prendre en considération d'autant plus rapidement que de nouveaux entrants s'ingénient d'ores et déjà les satisfaire. C'est le cas de PayPal et, beaucoup plus récemment, de fintech [startups spécialisées dans les technologies financières ; Ndlr] comme TransferWise. Ces nouveaux concurrents, dont l'émergence est favorisée par la directive européenne sur les services de paiement (DSP2), notamment, opèrent principalement sur le marché des transferts d'argent internationaux entre particuliers.

Mais Thierry Chilos, chez Swift, ne se fait aucune illusion : « Ces nouveaux acteurs vont venir sur le segment B2B (business to business), car il représente 80% à 85% des revenus que les banques tirent du marché des paiements internationaux. »

De fait, il n'y a pas de commune mesure entre les quelques milliers d'euros adressés par une personne émigrée à sa famille restée au pays, et les dizaines ou centaines de millions d'euros que s'échangent des multinationales. Un potentiel auquel Western Union, acteur traditionnel des transferts d'argent entre particuliers, s'intéresse également.

La blockchain, complémentaire de Swift

Face à cette menace, Swift a lancé en décembre 2015 un projet d'innovation visant à améliorer les éléments pointés du doigt par ses utilisateurs, projet qui a été adopté par 45 banques dans le monde, parmi lesquelles figurent trois établissements français, à savoir BNP Paribas, la Société générale et Natixis (groupe BPCE). L'un des objectifs étant par exemple de ramener à une journée le délai de réception des fonds. Un pilote, porté par 21 banques, dont une Française (BNP Paribas), vient d'être mis en place. Il portera dans un premier temps sur le marché B2B des paiements internationaux, avant d'être sans doute étendu au transfert d'argent entre particuliers. Swift dévoilera les résultats de cette expérimentation à l'automne prochain, au cours de l'édition 2016 de son salon Sibos, qui se tiendra à Genève.

Des résultats qui, comme la coopérative l'espère, pourraient convaincre bien d'autres banques de rallier ce projet de modernisation des paiements internationaux. Et ce, d'autant plus qu'il « *ne nécessitera pas d'investissements technologiques de la part des banques, mais (seulement) une amélioration de leurs processus internes, de leur back-office* », assure Stanley Wachs, directeur international de l'innovation des paiements chez Swift. Parallèlement, cette dernière lancera à partir du mois de juin des ateliers de réflexion sur la façon dont les technologies de rupture telles que la blockchain pourraient aider à réinventer les paiements interbancaires internationaux, dans les cinq prochaines années. La blockchain, cette technologie ouverte et libre, qui permet la circulation de monnaies cryptées comme le Bitcoin, est *complémentaire de Swift* », estime Stanley Wachs. Complémentaire et non pas concurrente, « *la blockchain n'apportant pas du tout le même niveau de sécurité que Swift, puisqu'elle ne possède pas, par exemple, les capacités de lutte contre le blanchiment dont les banques disposent* », insiste Stanley Wachs. 14/03/2016

Liens : <http://www.latribune.fr/entreprises-finance/banques-finance/industrie-financiere/les-banques-organisent-la-riposte-face-aux-fintech-dans-les-transferts-d-argent-556444.html>

#FinTech

L'avenir du secteur du transfert d'argent

De nouveaux acteurs bousculent le secteur du transfert d'argent et oblige le leader historique Western Union à élargir son offre. Devenu un réflexe pour le grand public lorsque l'envoi d'argent à l'étranger était évoqué, Western Union voit aujourd'hui sa domination remise en cause par des startups FinTech. Ce mastodonte, qui réalise un chiffre d'affaires de 5,7 milliards de dollars (en 2012), contrôle avec MoneyGram 50% du marché des transferts d'argent du continent africain avec des commissions les plus élevées du secteur (12% environ).

Leader historique du marché, Western Union a augmenté depuis 2009 ses partenariats et a élargi son offre multicanale, notamment via la possibilité de transférer de l'argent en ligne et vers des comptes mobiles.

Ce qui a influencé Western Union à se repositionner

Depuis 2009, il n'est plus nécessaire de disposer d'une licence bancaire dans l'exercice de cette activité. Cela a donc favorisé dans un premier temps, l'entrée de nouveaux acteurs comme TransfertWise et WorldRemit bousculant le secteur jusqu'alors emblématique, grâce à la technologie et avec une promesse simple : le rendre plus efficace, rapide et moins coûteux. WorldRemit a finalisé une levée de 100M\$ aux Etats-Unis il y a quelques mois. Pour en savoir plus à propos de ce marché et des évolutions à venir, la rédaction de Maddyness est allée à la rencontre de son fondateur.

Quels sont les chiffres clés de WorldRemit à ce jour ?

Aujourd'hui, WorldRemit réalise un quart de millions de transactions par mois. En 2013, nous avons enregistré un CA de 9.3 millions de dollars. Suite à une très forte croissance, nous avons eu le plaisir d'annoncer un CA de 25 millions de dollars en 2014.

Vous avez levé récemment 100 millions de dollars : à quoi l'argent va-t-il servir ?

L'investissement que l'on a reçu de Technology Crossover Ventures (TCV) va nous aider à devenir d'une part le leader mondial des transferts d'argent en ligne et d'autre part un challenger dans le secteur des versements d'argent, au beau milieu de Western Union et de MoneyGram.

Nous voulons multiplier nos partenariats avec les banques et les opérateurs mobiles dans le monde. Nous souhaitons couvrir davantage de pays et développer d'autres façons de transférer de l'argent. Par ailleurs, notre base de données s'agrandit de plus en plus. Nous mettons un point d'honneur à renforcer nos équipes de relations clients dans tous nos bureaux internationaux.

Quelle est votre vision du marché du transfert d'argent à long terme?

Avec l'évolution grandissante du transfert d'argent, c'est encore plus surprenant qu'uniquement une petite parcelle de transferts a été envoyée par internet.

Selon la banque mondiale en 2014, l'ensemble des transactions réalisé par des personnes depuis leur domicile représente l'équivalent de la moitié d'un trillion de dollars dans le monde entier.

Seulement 5% des transactions ont été réalisées sur internet. C'est donc pour nous une énorme opportunité de business. Notre vision à long terme serait de prendre le marché online et devenir le leader international des versements d'argents entre particuliers.

Quelle est votre « Secret Sauce » ?

Dès le départ, nous avons vu dans WorldRemit une réelle opportunité. Je pense que notre secret est que l'on a toujours considéré WorldRemit comme une « one-world solution » de transferts d'argent plutôt comme une entreprise globale divisée en différents départements.

Nous nous sommes aperçus que le transfert d'argent en Afrique était peu ou mal considéré par la concurrence et qu'il y avait pour nous une grande opportunité de ce côté-là.

Mais nous ne sommes pas arrêtés là. Nous avons prouvé que nous pouvions nous internationaliser notamment avec le bureau que nous avons ouvert aux Etats-Unis l'année dernière.

Où voyez-vous votre secteur d'activité dans 5 ans?

Le futur du secteur du transfert d'argent est inéluctablement en ligne, par conséquent sur nos mobiles. WorldRemit aura un tour d'avance dans 5 ans car nous permettons déjà de transférer de l'argent de mobile à mobile. La moitié de nos transactions se réalisent d'ores et déjà via nos applications IOS ou Android et via le net sur notre version mobile. Par ailleurs, nous continuerons de développer des services de paiement sur mobiles et rendre le transfert d'argent plus pratique pour les clients.

Selon vous, quelle sera la tendance sur les moyens de transactions et les systèmes de paiements dans le futur et quel en sera l'impact pour WorldRemit ?

Avant, envoyer de l'argent était peu pratique, obligeant de déposer l'argent chez des agences et d'attendre longtemps. En plus, le service clients était quasi inexistant. Mais tout ne doit pas être comme ça.

Chez WorldRemit, nous réalisons des transferts d'argent en ligne. Cela signifie que nous offrons un service plus rapide, avec un grand nombre de transactions qui arrivent instantanément sur les comptes bancaires et les comptes sur mobiles.

Etre en ligne signifie également que l'on a une meilleure couverture des préventions des fraudes que des agents traditionnels de transfert d'argent. Il est également plus facile de faire des contrôles en ligne qu'avec des espèces.

Vous êtes en train d'innover la façon dont on transfère de l'argent qui est déjà très compétitif et est un secteur saturé, quelle est votre point de vue sur la tendance autour de la politique de prix?

Depuis des années, des entreprises implantées dans le secteur telles que Western Union ou MoneyGram ont imposé des commissions excessives et ont passé des accords avec les agents. L'année dernière, L'Africa Progress Panel – dirigé par Kofi Annan – a dénoncé ces pratiques en Afrique.

Depuis avec l'appui du G8 et du G20, ils ont l'intention de réduire les coûts des transactions. Notre mission chez WorldRemit est d'insister sur le transfert d'argent duopole et d'offrir des prix intéressants à nos clients.

Quels sont vos business modèles sur le long terme?

WorldRemit a en commun avec de nombreux services innovants, l'utilisation existante de la technologie mise à sa disposition dans le monde. Dans notre cas, on a cherché des milliers de systèmes financiers et nous les avons articulés ensemble de façon à ce qu'ils forment une seule et même plateforme.

Quel est votre positionnement face à des nouveaux acteurs comme Transferwise?

On est souvent cité à leur côté, mais nous ciblons 2 types de clients totalement différents. Transferwise est sur l'environnement du FX* (Forex ou marché des changes) et nous sur le transfert d'argent international. Il y a peu de similitudes.

*FX: Le forex est le marché des changes ou devises. *“Le marché sur lequel des devises du monde entier sont échangées l'une contre l'autre, à des taux de change qui varient sans cesse. Sur ce marché mondial, toutes les monnaies sont vendues et achetées en temps réel”.*
Définition infinance.fr

Quel est votre argument commercial?

En tant que business en ligne, on a été très actif dans l'acquisition de nouveaux clients en ligne partout dans le monde. De notre expérience, nous comptons aussi sur nos clients pour faire le relais : Plus de 70% de nos clients reviennent utiliser nos services et nombreux d'entre eux recommandent WorldRemit à leur entourage familiale et amicale basée sur l'expérience satisfaisante qu'ils ont eu avec nos services. Nous avons également investi davantage de temps et d'énergie sur le transfert via mobile (d'un smartphone vers un compte Mobile Money) que d'autres sociétés.

Avez-vous une stratégie spécifique de segmentation pour les pays comme l'Inde, la Chine ou les Philippines?

WorldRemit est un service global et différent de nos concurrents. On permet de transférer de l'argent et d'apporter de la valeur ajoutée dans des endroits mal desservis. Nous développons continuellement notre empreinte dans le secteur du versement d'argent.

Quelle est votre cible dans les pays émergents (ouvriers, personne n'ayant pas de comptes bancaires...)?

Les gens envoient de l'argent de chez eux pour plusieurs raisons?: aussi bien pour payer leurs factures que leur voyage, leur loyer ou payer des frais hospitaliers ou pour des écoles et leurs études. Dans de nombreux cas nous n'avons pas de «cibles?» spécifiques. Si vous avez besoin d'envoyer de l'argent à vos amis ou à votre famille, l'équipe de WorldRemit est disponible pour vous accompagner dans vos démarches. Le fait que nous réalisons des transactions dans des pays émergents est l'une de nos plus grandes satisfactions dans notre business.

Il y a plus de 2.5 milliards de personnes dans le monde qui n'ont pas accès à des services financiers dont 1 milliard qui possède un téléphone portable. C'est un champ de possibilités très important pour nous.

Comment évaluez-vous le blanchiment d'argent en termes de risque pour votre métier sur le long terme?

WorldRemit a été créé sur une grosse plateforme pour veiller aux aspects de conformité et de déontologie.

En tant qu'ancien conseiller auprès des Nations Unies, je sais que les problèmes liés au blanchiment d'argent et la régulation liée au financement du terrorisme peuvent être très contraignantes pour les sociétés de transfert d'argent. Nous avons une équipe d'experts dédiée afin de répondre aux exigences des systèmes de régulations financières dans tous les pays dans lesquels nous opérons.

Comment gérez-vous le problème du blanchiment d'argent en particulier aux Etats-Unis, en France et au Royaume-Uni ?

Notre groupe de directeurs qui veillent à ses problématiques est basé à Denver afin de superviser les entretiens avec le système de régulation et de toutes les problématiques dans tous les Etats-Unis. Avec les directeurs internationaux et les managers de «conformité?» nous avons toute l'expertise nécessaire afin de répondre à n'importe quelle demande du régulateur. Nous avons été approuvés par le régulateur financier du Royaume-Uni (FCA) et sommes soumis aux mêmes restrictions que n'importe quel opérateur financier.

Quelle stratégie avez-vous mis en place autour du conflit d'intérêt sur vos clients/utilisateurs?

WorldRemit est soumis aux lois de "connaître son client – Know Your Client" (KYC) afin de prévenir d'attaques frauduleuses de notre plateforme. Nous vérifions l'identité de nos clients et enregistrons toutes nos transactions. En tant que "digital service", nous avons construit un algorithme puissant et complexe qui permet de détecter les fraudes. Nous sommes mieux informés pour les régulations et conflit d'intérêt que n'importe quelle entreprise de transfert d'argent.

Vous êtes un grand admirateur de Steve Jobs? Qu'avez-vous appris de lui qui vous aide dans votre business?

Steve Jobs était un entrepreneur extraordinaire. Il avait cette capacité à savoir ce que les gens comme vous et moi voulaient avant que l'on ne le sache nous-même. Il pouvait savoir ce qu'il se passait de l'autre côté de la montagne et surprendre les autres avec une extrême attention aux détails. Sa vision s'alliait aux tendances du comportement humain et de la technologie comme personne, ce qui lui a permis d'avoir une stature unique pour conduire son entreprise vers le succès.

Liens : <https://www.maddyness.com/innovation/2015/04/10/worldremit-ismail-ahmed/>

Richard Branson investit 25 millions de dollars dans la start-up de transfert de fonds TransferWise

Il y a quelques mois, la start-up TransferWise gagnait en visibilité en annonçant le transfert d'un milliard de livres sterling sur sa plate-forme.

Avec Sir, Richard Branson vient d'investir avec quelques autres 25 millions de dollars (soit 18 459 750 € d'après le taux équitable de TransferWise au moment de l'écriture de cet article) elle franchit un deuxième jalon en relations publiques.

Une partie de cet argent serait d'ailleurs destinée à une campagne de publicité, à laquelle Branson pourrait participer. D'après le CEO, la start-up pourrait déjà être rentable, mais préfère investir dans sa croissance. Au total, la start-up aura reçu 31 millions d'euros de fonds depuis sa création.

Créée, il y a trois ans par deux estoniens, cette entreprise permet de transférer des fonds à l'étranger en prenant une commission de 0,5 % (1 € au minimum pour des transferts de 200 € ou moins).

L'offre

Ce qui est nettement moins cher que la même opération réalisée auprès d'une banque. Car même quand une banque affirme qu'elle ne fait pas payer de frais, elle prend une commission non négligeable sur les taux de change, commission qui peut avoisiner les 5 %. Pour la start-up, il n'y a qu'un taux juste, et c'est le taux interbancaire.

Le client peut donc réaliser jusqu'à 90 % d'économies. Elle donne l'exemple d'un transfert de 1000 £ qui rapporterait 1 231 € avec son service contre 1 176 € avec une banque typique, soit 55 € d'économies.

La firme communique d'ailleurs sur ces frais cachés avec agressivité en Angleterre, ce qui lui a valu quelques problèmes avec les autorités de régulation de la publicité. Elle regrette que cette autorité ne comprenne pas toujours le fonctionnement des transferts.

Quoi qu'il en soit, la start-up garantit le taux effectif le meilleur pour le client, et s'engage à s'aligner si le client trouve un taux plus avantageux.

À l'heure actuelle, la majorité de ses 10 000 clients sont basés au Danemark, en Pologne, au Royaume-Uni, en Suède et en Suisse.

Le secret des taux bas

Comment la start-up peut-elle proposer des taux aussi bas ? En fait, elle n'échange pas d'argent.

Quand un client français veut envoyer 1 000 € à sa tante aux États-Unis, il vire l'argent sur le compte de la filiale française de TransferWise. Le système de la start-up recherche alors un client américain qui veut faire une transaction en sens inverse, peut-être pour son grand-père français, et qui dépose des dollars dans sa filiale américaine. Elle opère alors un transfert de la filiale américaine pour créditer le compte de la tante, au taux interbancaire, et un transfert de la filiale française pour créditer le compte du grand-père, au taux interbancaire inverse.

En d'autres termes, l'argent ne franchit pas les frontières.

C'est ce que le cofondateur et président Taavet Hinrikus aime comparer à Skype, lui qui en était l'un des premiers employés.

Les limites

La limite du système est que les transferts doivent être relativement symétriques entre deux zones. Dans le cas d'un pays, qui accueillerait beaucoup plus d'immigrés qu'elle n'a d'émigrés, on peut penser que les transferts seront essentiellement unilatéraux, ces derniers envoyant de l'argent à leur famille au pays natal.

Notons d'une part que ce système pourrait aider au blanchiment d'argent, dans la mesure où les régulations sur les transferts nationaux sont souvent moins contraignantes que les transferts internationaux. Et, d'autre part, qu'il n'est pas interdit de penser que certaines banques utilisent un système similaire, au moins en partie.

Liens : <http://www.lediligent.com/2014/06/10/richard-branson-investit-25-millions-de-dollars-dans-la-start-up-de-transfert-de-fonds-transferwise/>

Paiement en ligne Etat des lieux en Belgique

Quels moyens de paiement sont les plus appropriés pour un site de commerce électronique? Quels sont leurs avantages et inconvénients ?

De nombreux sites de commerce électronique nécessitent la mise en place de solutions de paiements électroniques, surtout en BtoC (vente vers le consommateur final), le vendeur souhaitant recevoir la confirmation du paiement avant de livrer le produit ou fournir le service demandé.

Au balbutiement du commerce électronique, de nombreux sites se contentaient de recueillir les numéros de cartes de crédit des clients via un simple formulaire en ligne, procédé particulièrement peu fiable pour le client, dont la carte de crédit pouvait être débitée par une personne malintentionnée qui avait repéré le numéro lors du transfert, mais aussi pour le commerçant: celui-ci n'avait pas de certitude que le détenteur effectif de la carte était bien celui qui passe commande. De plus, les données bancaires étant stockées sur son serveur raccordé à internet, le cybercommerçant risquait d'être victime d'un acte de piratage. D'où l'apparition d'une certaine méfiance autour des paiements sur Internet

Ces méthodes sont maintenant heureusement révolues, avec le développement d'autres moyens de paiement que la carte de crédit, la généralisation de systèmes de contrôle permettant d'éviter l'usurpation de cartes de crédit, et surtout avec l'apparition de sociétés spécialisées dans la gestion des transactions de paiement électronique assurant un rôle de tiers de confiance, les « Payment Service Providers » (PSP).

Quelles sont les différentes solutions qui se présentent à l'heure actuelle en Belgique ?

a) Paiements immédiats, en ligne

Il existe différentes formules de paiement en ligne: carte de crédit, carte de crédit jetable, paiement à débit immédiat (cartes de débit et transferts électroniques), paiement par e-mail ou via des comptes de tiers, communications surfacturées, paiements mobiles

1. La carte de crédit

C'est le moyen de paiement en ligne numéro 1, grâce à sa simplicité et son universalité, mais que le cybercommerçant doit accepter avec prudence.

Avantages :

- **simplicité:** nécessité juste de recueillir un numéro de code, un nom et prénom, une date de validité, et un code de vérification, informations qui se trouvent sous une structure identique sur toutes les cartes du monde;
- **universalité:** possibilité de réceptionner des paiements quelque soit le pays d'origine de l'acheteur, sans se soucier des éventuelles opérations de change nécessaires;
- **paiement différé au niveau du consommateur:** élément favorisant bien évidemment les achats impulsifs.

Inconvénients:

- **public restreint** aux personnes majeures, ayant généralement dû justifier de revenus réguliers pour recevoir une carte de crédit. Il y a néanmoins environ 3 millions de

cartes en circulation en Belgique (dont plus de 90% émises par l'acquéreur Bank Card Company);

- usuration (de moins en moins) aisée: la simplicité du dispositif engendre la possibilité pour toute personne ayant noté les numéros de la carte d'un tiers d'effectuer des opérations sur le compte de celui-ci. Ce risque n'est évidemment pas lié au commerce électronique, de telles opérations pouvant aussi être effectuées par fax ou téléphone;
- coûts des commissions sur les transactions perçus par l'acquéreur et par le PSP. Ils sont variables selon le contrat, dans un ordre de grandeur de 0,8 à 2,5%, plus souvent un montant fixe par mois, plus un coût fixe par transaction
- les transactions sont plafonnées à un certain montant total de dépenses par mois. Généralement, il s'agit par défaut de 1250 euros. Ainsi, ce mode de paiement est inapproprié pour la vente de produits d'un montant supérieur et ne devrait pas être le seul proposé aux clients si le panier moyen attendu dépasse les 500 euros.

Aussi, surtout si le site s'adresse à un public international, la carte de crédit reste un des principaux moyens de paiement à proposer sur un site Internet.

La carte de crédit jetable

Une formule alternative consiste à utiliser une carte de crédit « jetable ».

Compte tenu du climat de méfiance autour du paiement par carte de crédit apparu au début du commerce électronique, plusieurs banques ont imaginé le concept de carte de crédit virtuelle de manière à rassurer le client: ainsi, au lieu de taper son propre numéro de carte de crédit, le consommateur encode en ligne un autre numéro qui est:

- soit éphémère (valable pour une seule transaction),
- soit permanent, mais dont le consommateur peut modifier à tout moment le montant maximum utilisable et parfois d'autres limites (par exemple valable dans un seul pays).

Ce compte virtuel est lié à une carte de crédit classique ou bien à un compte bancaire, mais le couplage n'est connu que de la banque et du client.

Ce moyen de paiement était anecdotique en Belgique jusqu'à l'arrivée sur le marché, fin 2011, de la carte prépayé « B-Paid » lancée par la Poste. Cette carte, commercialisée au prix de 12 euros par an, rechargeable en ligne, par virement, ou par dépôt dans un bureau de Poste, est utilisable dans toutes les boutiques en ligne proposant « Mastercard Secure ». D'autres banques ont lancé depuis des solutions équivalentes.

D'autres formules ne sont acceptées que sur certains sites d'e-commerce adaptés en fonction. Ce procédé limite dès lors souvent l'usage aux pays où la banque est présente et aux cybercommerçants avec lesquels elle a conclu un accord.

Ce mode de paiement peut être pertinent pour les sites de commerce électronique s'adressant à des profils d'acheteurs novices en commerce électronique et plutôt méfiants, à des consommateurs mineurs, ou lorsque l'acheteur potentiel souhaite conserver l'anonymat. En effet, avec ce procédé, généralement seule la banque émettrice dispose du nom du client.

A noter que ce mode de paiement n'est pas approprié par rapport à la carte de crédit traditionnelle lorsque la réservation ou les achats nécessitent de présenter la carte qui a été utilisée (par exemple pour retirer des tickets).

2. Méthodes de virements électroniques pré-remplis

Ce moyen de paiement national est bien adapté au BtoC, mais aussi au BtoB.

A l'origine, plusieurs banques belges importantes ont développé leur propre système permettant de valider en ligne des virements pré-remplis d'un de leurs comptes à un autre. Ce système se basait parfois sur l'outil de Web-banking « maison » ou sur une plate-forme électronique spécifique. Il pouvait donc être utilisé par tout client de banque qui s'était abonné à ce service, moyennant parfois un contrat supplémentaire. Le client était redirigé vers cet

outil en cliquant sur le bouton correspondant à sa banque affiché sur le site d'e-commerce. Il validait ensuite un virement électronique (pré-rempli) qui transférait le montant sur le compte du vendeur.

Chaque banque ayant son propre système (CBC/KBC Online, Belfius NetBanking, ING Home'Pay), le cybercommerçant devait souscrire à un abonnement auprès de chacune d'entre elles et adapter son site de commerce électronique afin de pouvoir accueillir l'ensemble des clients de ces différentes banques (sauf s'il faisait appel à un PSP qui intégrait les différentes solutions des banques dans sa solution). Dès lors, peu de cybercommerçants ont proposé ce mode de paiement, et donc peu de clients ont souhaité disposer de ce service auprès de leur banque. Ce mode de paiement est donc resté peu utilisé, jusqu'à ce que le secteur bancaire belge, inquiet de la prépondérance des paiements par cartes de crédit, tente de reprendre des parts de marché. Il s'est repositionné via, cette fois-ci, une solution commune aux principales banques belges actives en ligne, basée sur la carte de débit classique Bancontact-MisterCash déployée par Atos Worldline (ex-Banksys).

Service « Bouton Bancontact »

Lors de l'étape « paiement », le navigateur Internet de l'acheteur est redirigé vers l'interface de Web-banking de sa banque, auquel il est généralement familiarisé. Il encode le numéro de la carte de débit, c'est-à-dire un nouveau numéro PAN (Primary Account Number), comportant 17 chiffres et commençant par 6703. Le titulaire valide l'opération de la même manière qu'il effectue d'ordinaire ses transactions bancaires en ligne (selon les banques, via par exemple une calculette « digipass », etc.). Cette redirection permet de s'assurer que l'acheteur est bien le titulaire de la carte.

Le cybercommerçant devra payer une commission par transaction (compris entre 1 et 1,5%), mais aussi des frais d'abonnement et de transaction auprès du prestataire qu'il aura choisi pour implémenter le programme de capture et de suivi des commandes sur son site Internet.

Avantages:

- sécurité des transactions: celles-ci s'effectuent avec le même niveau de sécurité que les opérations bancaires en ligne. Le risque de piratage est très faible;
- non répudiation possible: l'usage à l'interface de Web-banking est personnel, protégé par un mot de passe;
- la carte de débit est fort répandue: plus de 10 millions d'exemplaires en Belgique, les belges en ayant plusieurs. Ainsi le site d'e-commerce peut atteindre une population plus large: les adolescents, les retraités et les sans-emplois.
- pas d'apprentissage nouveau pour les personnes déjà habituées à effectuer des opérations bancaires en ligne. Celles-ci seront donc assez facilement disposées à utiliser ce mode de paiement;
- pas de plafond mensuel: la transaction sera acceptée du moment que le compte bancaire est suffisamment alimenté ou que l'ouverture de crédit à la consommation qui aurait été accordée à ce client est suffisante. Toutefois, des plafonds sont parfois fixés dans le contrat de Web-banking;
- bonne adaptation aux transactions BtoB (entre sociétés), l'usage de la banque en ligne se généralisant dans les entreprises.

Inconvénients:

- non universalité: il s'agit d'un système de portée nationale pour l'instant, mais qui devrait s'élargir dans le cadre du SEPA (Single Euro Payments Area, zone de paiement européenne unique). De plus, tous les clients des banques n'ont pas souscrit à un abonnement de Web-banking, qui fait parfois l'objet d'un supplément;
- contestation difficile: contrairement au paiement par carte de crédit qui applique un remboursement direct en cas de contestation, avec charge pour le vendeur de montrer

qu'il y a une fraude, le client devra introduire un dossier pour être remboursé s'il n'a pas reçu le produit et n'a pas été directement remboursé par le vendeur.

Ce mode de paiement rencontre un fort développement en Belgique, atteignant maintenant de l'ordre de 1/5 des paiements électroniques en ligne.

Il est plus particulièrement recommandé lorsque le site s'adresse particulièrement aux jeunes, ou bien à d'autres sociétés (BtoB), lorsque le panier moyen est d'au moins 10 euros.

A noter l'apparition d'une concurrence, dans le chef de Maestro, qui ne fonctionne toutefois actuellement, pas avec les cartes de débit Maestro émises par certaines (petites) banques belges.

3. Systèmes de paiement par e-mail ou via des comptes virtuels de tiers

Il s'agit de systèmes de paiement très faciles à mettre en place et de portée internationale, mais à l'origine surtout conçus par les transactions CtoC. Le marché du paiement électronique présente de grandes opportunités d'affaires au niveau mondial de sorte que plusieurs sociétés multinationales se sont positionnées dans ce créneau.

Il en est ainsi de la société eBAY qui a racheté la société « PayPal », concepteur d'un système de paiement sous cette dénomination.

Ce système s'inspire du principe des cartes virtuelles: il couple un moyen de paiement classique, comme une carte de crédit, à un identifiant auquel est associé un mot de passe. Une fois inscrit (en communiquant par exemple un numéro de carte de crédit), le client peut effectuer des transferts d'argent auprès de toute autre personne disposant aussi d'un compte « PayPal », en communiquant l'identifiant (dans le cas de Paypal, une adresse e-mail) et le mot de passe. Il est possible de payer, mais aussi de recevoir de l'argent.

Il présente les mêmes avantages et les mêmes inconvénients que le moyen de paiement auquel il est généralement couplé, la carte de crédit. On notera surtout que PayPal est un moyen de transfert financier de portée internationale, simple (il est facile de s'inscrire et de l'utiliser, avec juste un login et un mot de passe), accepté par un très grand nombre de marchands et auquel plus de 200 de millions de personnes ont souscrit.

De plus, il n'y a pas de frais d'installation, d'abonnement mensuel, de frais d'installation de passerelles techniques etc.

Le système n'est pas par contre incomparablement moins sûr que le paiement par virement pré-rempli, validé par un code unique généré par exemple par un Digipass: Il ne s'appuie que sur un couplage « login + mot de passe », que des personnes malintentionnées peuvent tenter de recueillir auprès des utilisateurs par phishing notamment, en se faisant passer pour le service d'assistance de Paypal...

En effet, dans certaines régions du monde, l'ouverture d'un compte virtuel n'est pas aussi contrôlé que l'attribution d'une carte de crédit, notamment au niveau de l'identité du détenteur. De sorte que ce mode de paiement doit être utilisé avec prudence lorsqu'il s'agit de verser de l'argent à un individu que l'on ne connaît pas ou à une société qui n'a pas pignon sur rue. Pour compenser cette faiblesse importante au niveau de l'authentification des deux parties, PayPal inclut dans les frais de commission perçus (3,4% en Belgique actuellement, plus 0,35 euro et une éventuelle marge de change de 2,5%) une assurance qui couvre les transactions jusqu'à un certain montant (actuellement 500 euros).

Les sociétés spécialisées Ogone et Neos Solution peuvent intégrer PayPal sur un site d'e-commerce. En Europe, PayPal est utilisé dans plus de 30% des cas pour des transferts financiers sans lien avec eBay.

A noter que les micro-paiements (à partir même de 0,01 euros) sont généralement bien assurés par ces systèmes.

Un mot enfin sur le système « Western Union ». Il s'agit d'un système de transferts de fonds, d'une personne à une autre, basé sur un nombre très important d'agences à travers le monde. Il est bien adapté par exemple pour verser de l'argent à des proches résidant à l'étranger,

surtout dans des pays où l'accès aux services bancaires n'est pas généralisé. Par contre, il ne convient pas pour le commerce électronique et encore moins pour le paiement en « CtoC », auprès de personnes qui ne sont pas connues du donneur. Un vendeur qui ne permet qu'un paiement via ce système doit inspirer une grande méfiance. Ainsi, en Belgique, une très large majorité des plaintes pour escroqueries et arnaques via Internet proviennent de personnes qui ont versé de l'argent via Western Union à des inconnus.

4. Les codes uniques, prépayés

Ces cartes prépayées peuvent être achetées en magasin (réseau de boutiques affiliées), ainsi qu'en ligne ou par virement bancaire. L'internaute doit gratter les chiffres au dos de la carte (ou télécharger ce code sur un site web). En tapant ce code unique, il est alors possible d'accéder à des services Premium de réseaux sociaux, de consulter des documents en archives, de télécharger des logiciels, de jouer en ligne,...

Ces dispositifs ne sont pas liés automatiquement à un compte bancaire et présentent généralement un anonymat bancaire. Ils sont simples d'utilisation, s'adressent plus particulièrement à un public non ou peu bancarisé, et sont très adaptés aux petits montants d'achats (moins de 5 euros) ainsi qu'à la fourniture de biens dématérialisés (ex: jeux en ligne). Par contre, ils présentent l'inconvénient qu'il est nécessaire pour l'acheteur d'acquérir des codes préalablement.

Les monnaies virtuelles

A noter également, le développement de monnaies virtuelles, en circulation uniquement en ligne. ex:

Webmoney, Ukash, Bitcoins,...

Au stade actuel, des monnaies virtuelles doivent être acceptées avec grande prudence par les e-commerçants, les cours de ces monnaies pouvant varier fortement et ces monnaies étant parfois utilisées comme moyen de blanchir de l'argent.

B) Paiements immédiats, via GSM:

Transfert validé par une application mobile

Les principales plateformes d'applications pour smartphone (sous iOS, Android, Windows Phone) proposent maintenant des solutions à installer sur son GSM, qui permettent à l'utilisateur,

- soit de signer électroniquement un virement (en employant en parallèle un Digipass; ex: l'application « scasher » de KBC),
- soit de valider un transfert financier d'un portefeuille virtuel à un autre (ex: Paypal).

En Belgique, les paiements par mobile restent toutefois actuellement marginaux (de l'ordre de 1% des paiements en e-commerce, hors achat d'applications / logiciels). Ils sont surtout employés pour l'achat de tickets / vouchers virtuels.

C) Paiements en différé

Si en BtoC, le client n'étant généralement pas connu du vendeur, la prudence voudrait que le paiement soit exigé avant livraison, le paiement en ligne n'est pas pour autant incontournable.

A côté des « véritables » moyens de paiement électronique en ligne, pour donner confiance au consommateur et réduire le pourcentage élevé d'abandons de commandes au stade du paiement, il est recommandé de proposer sur un site d'e-commerce au moins une formule de paiement « off-line »

1. Paiement contre livraison

Il s'agit d'une solution coûteuse, mais rassurante, tant pour le client que pour le vendeur. Cette formule très classique permet au client de régler le montant de l'achat auprès du livreur, au moment de la livraison ou lors du retrait dans un point de livraison (exemple: les points de vente affiliés au réseau Kiala ou au réseau Mondial Relay).

Avantages:

- Rassurant pour les 2 parties: le vendeur ne prend pas le risque de livrer de la marchandise sans être sûr d'être payé. L'acheteur ne prend pas le risque de payer de la marchandise qu'il n'est pas certain de recevoir;
- Pas de contestation possible concernant la livraison;
- Simplicité technique: Pas d'installation technique particulière à prévoir sur son site Internet;
- Service pouvant être international (en fonction de la société de livraison sélectionnée)

Inconvénients:

- Nécessité pour l'acheteur d'être présent lors de la livraison. L'acheteur doit disposer à ce moment de liquidités pour régler le livreur, celui-ci n'étant pas systématiquement équipé d'un terminal mobile de paiement bancaire. Certains prestataires logistiques offrent la possibilité de retirer l'article auprès de points d'enlèvement (station essence, librairies, supermarché, etc.) où le paiement s'effectuera classiquement à la caisse;
- Commission importante perçue par le prestataire de livraison pour ce service, surtout au niveau international;
- Risque d'une plus grande proportion de commandes bidons ou refusées lors de la livraison, ce qui peut entraîner pour le cybercommerçant des frais de livraison et de retour de marchandises non couverts;
- Ne convient évidemment pas pour la fourniture de produits dématérialisés (fichiers musicaux, etc.)

Ce mode de paiement est particulièrement adapté pour la vente de produits, d'une certaine valeur (entre 20 et 1 000 euros), qui doivent être livrés aux clients. Aussi, dans ce cas, il est recommandé de proposer cette formule en plus des modes de paiement en ligne, éventuellement moyennant un supplément.

2. Paiement par virement bancaire

Cette solution est la moins chère, mais elle est évidemment risquée pour le vendeur. Le client effectue un virement bancaire ordinaire sur le compte bancaire du vendeur. Il existe deux possibilités.

a) Soit le vendeur exige que le montant lui parvienne pour que la livraison soit effectuée.

Avantages:

- Gratuité du virement bancaire (ou très faible coût au niveau européen) tant pour l'acheteur que pour le vendeur;
- Fiabilité par rapport à d'autres moyens de paiement traditionnels, tels que le chèque.

Inconvénients:

- Non immédiateté. Plusieurs jours peuvent s'écouler, voire plus d'une semaine lors de virements internationaux (hors format normalisé « européen »), avant que l'argent ne parvienne sur le compte du vendeur;
- L'acheteur doit faire confiance au vendeur quant à la livraison. De plus, celle-ci sera retardée, le vendeur attendant d'être payé avant de fournir le produit ou service demandé;
- Coût important pour les transactions de/vers des pays hors Union Européenne.
- b) Soit le vendeur demande au client de payer après réception, au terme du délai de réflexion.

3. Factures

La facture est la solution incontournable en Business to Business. Celle-ci est traditionnellement établie sous format papier, mais peut maintenant légalement se présenter sous format électronique, évolution qui facilite le traitement administratif tant pour le commerçant que pour l'acheteur.

Certes, ce mode de paiement n'est pas le plus recommandé pour un site orienté vers une clientèle nouvelle, compte tenu du risque par le cybercommerçant de non paiement de la marchandise livrée. Si ce risque est significatif, la formule « livraison contre paiement » est plus appropriée.

Liens : <http://www.retis.be/comment-vendre-en-ligne/parcours-client/servir/paiement/>

"Les monnaies virtuelles favorisent le risque d'escroquerie "

"Les monnaies virtuelles, qui s'achètent sur des plates-formes web et servent de moyens de paiement sur certains sites internet, ne sont pas contrôlées par les banques et échappent à la plupart des formes de régulation. Le risque de fraude et de blanchiment, mais aussi d'escroquerie est donc fort", affirme Jean-Baptiste Carpentier, directeur de Tracfin, la cellule du ministère de l'Economie qui est en charge du renseignement sur les circuits financiers clandestins. (Sipa)

Interview- Pour Jean-Baptiste Carpentier, directeur de Tracfin, la cellule "anti-blanchiment" de Bercy, les monnaies virtuelles, ainsi que les cartes-prépayées et Monéo présentent un risque.

Jean-Baptiste Carpentier, directeur de Tracfin, la cellule du ministère de l'Economie qui est en charge du renseignement sur les circuits financiers clandestins, se dit inquiet après le scandale Liberty Reserve. Le 28 mai, la justice américaine a en effet démantelé la plus grande fraude financière jamais décelée sur internet. La société Liberty Reserve est accusée d'avoir blanchi, grâce à sa monnaie virtuelle du même nom, plus de 6 milliards de dollars (4,6 milliards d'euros) en sept ans. Selon Jean-Baptiste Carpentier, la France n'est pas à l'abri de ce type de risque. Il explique pourquoi.

Après le scandale Liberty Reserve aux Etats-Unis, craignez-vous que l'utilisation de monnaie virtuelle favorise le blanchiment d'argent ?

Oui. Je ne suis d'ailleurs pas du tout surpris par ce scandale, mais inquiet qu'une affaire semblable se produise en France. Car les monnaies virtuelles, qui s'achètent sur des plates-formes web et servent de moyens de paiement sur certains sites internet, ne sont pas contrôlées par les banques et échappent à la plupart des formes de régulation. Le risque de fraude et de blanchiment, mais aussi d'escroquerie est donc fort. En revanche, il convient de souligner que la monnaie électronique, c'est-à-dire les cartes prépayées ou le système Monéo, fait l'objet d'une régulation, issue de directives européennes et d'une loi française. Ces instruments sont légaux lorsqu'ils respectent cette régulation. Mais cette devise électronique constitue néanmoins un instrument à risque dans la mesure où elle favorise l'anonymat : en pratique, ces cartes peuvent devenir des « comptes au porteur », dont on ne connaît pas l'identité du détenteur. Or ces comptes ont justement été supprimés en France et à l'étranger, dans le cadre de la lutte anti-blanchiment. Sauf à limiter strictement l'emploi de ces cartes à des montants minimes, leur usage est donc largement contradictoire avec les mesures mises en oeuvre en ce domaine depuis plus de vingt ans.

Comment fonctionne le schéma de blanchiment par de la monnaie virtuelle ?

Je peux obtenir de la monnaie virtuelle, la liberty reserve par exemple, en l'achetant sur internet, souvent à l'étranger, via ma carte bancaire ou tout autre moyen de paiement. Ensuite j'achète n'importe quels produits, de la drogue ou des armes, que je paye avec cette monnaie virtuelle. L'argent est ainsi blanchi. Il est difficile de tracer les opérations, qui ne sont surveillées par personne.

Combien de cas avez-vous déjà repéré en France ? Tracfin a déjà détecté plusieurs cas. Nous en avons transmis certains à la justice, ces affaires sont en cours d'enquête. **Peut-on imaginer en France des affaires de l'ampleur de celle des Etats-Unis ?** En principe non,

les montants ne seront pas les mêmes, le marché n'a pas la même taille. Et les Français sont moins sensibles à ces nouveaux moyens de paiement, car l'économie est très bancarisée. La plupart des habitants possèdent un compte, contrairement à beaucoup d'autres pays. Nous sommes probablement moins exposés aux risques que les Américains.

Quel est le volume ou le montant des monnaies virtuelles et électroniques ?

Je n'avancerai aucun chiffre. C'est comme les données sur la délinquance, c'est très difficile à estimer. Mais les monnaies virtuelles et électroniques semblent être beaucoup plus développées à l'étranger, notamment en Russie ou aux Etats-Unis. Quoi qu'il en soit, c'est un sujet amené à prendre de l'ampleur. Dès 2011, Tracfin a tiré la sonnette d'alarme en France et auprès de la Commission européenne, qui avait adopté une logique très libérale sur la question. Notre rapport annuel indiquait clairement notre préoccupation sur les monnaies virtuelles et sur certains risques liés à la monnaie électronique. Je pense qu'on a laissé naître un système intrinsèquement dangereux.

Vous déconseillez aux Français l'usage de monnaie virtuelle, qui permet par exemple de diminuer les frais lors de l'envoi d'argent d'un pays à l'autre ?

Je n'ai pas à donner de conseil, mais l'affaire autour de la monnaie liberty reserve et les évolutions erratiques de la monnaie virtuelle la plus connue, le bitcoin, incitent à la prudence. Voir son compte saisi, parce qu'on ne savait pas qu'il y avait le FBI derrière, ou sa valeur diminuer en quelques heures n'est pas très rassurant ! Par ailleurs, l'opacité de beaucoup de ces monnaies peut favoriser des escroqueries au détriment du consommateur. Personnellement, je souhaite que les monnaies virtuelles soit régulées, voire interdites pour certaines d'entre elles.

Liens : <http://www.challenges.fr/economie/20130603.CHA0244/les-monnaies-virtuelles-favorisent-le-risque-d-escroquerie.html>

[Chiffrement] Après Apple, Whatsapp dans la ligne de mire ?

L'application de messagerie sécurisée Whatsapp serait la prochaine cible des autorités dans la guerre qu'elle mène contre la course au chiffrement des géants du web, révèle le *New York Times*.

Il n'est pas question d'iPhone, d'Apple ou de terrorisme ici, néanmoins le problème reste le même : le chiffrement.

Dans le cadre d'une enquête en cours, un juge fédéral américain a donné son feu vert aux autorités pour procéder aux écoutes des communications passées depuis l'application de messagerie sécurisée Whatsapp. Problème, avec le chiffrement de bout en bout des communications proposées par la société depuis 2014 cela se révèle compliqué et l'enquête stagne.

Le Département de la Justice (DOJ) étudierait donc actuellement des solutions de contournement et des pourparlers seraient engagés entre Whatsapp et le DOJ, rapporte le *New York Times*.

Toutefois, alors que le contexte est déjà tendu et voit Apple et le FBI se livrer une guerre de tranchées autour de la sécurité des données et des communications, des sources proches du dossier assurent que le problème est autrement plus préoccupant dans cette affaire.

Pour le *NYT*, cela ouvrirait « *un nouveau front dans la contestation entre l'administration Obama et la Silicon Valley autour du chiffrement, de la sécurité et de la vie privée* ». Avec le chiffrement, l'avenir des écoutes électroniques serait en jeu. Écoutes que les agences de renseignement estiment être à la base de toute enquête criminelle.

La question étant désormais de savoir si le Département de la Justice doit forcer Whatsapp à aider le gouvernement afin qu'il obtienne ces informations, au risque de voir s'aggraver le conflit. De leur côté, les sénateurs seraient sur le point de légiférer concernant les sanctions civiles à imposer aux entreprises high-tech, qui refuseraient de répondre aux ordonnances du tribunal requérant leur coopération pour aider les autorités à accéder aux données chiffrées de leurs utilisateurs.

Un conflit juridique avec Whatsapp pourrait également inciter les législateurs à réviser la loi sur les écoutes (*wiretapping*) dont la dernière mise à jour remonte à une génération.

Pour l'Electronic Frontier Foundation (EFF), le FBI et le ministère de la Justice attendent juste le moment et le cas opportuns pour effectuer une demande qui apparaîtrait enfin raisonnable.

Whatsapp n'est pas la seule application chiffrée existante – Telegram serait d'ailleurs privilégiée par les djihadistes de l'organisation Etat islamique (OEI) pour communiquer – mais avec 1 milliard d'utilisateurs, elle est, de loin, la plus importante.

Le chiffrement n'est pas qu'une sécurité pour les clients des géants du web, c'est aussi un moyen pour le gouvernement de se protéger des cyberattaques dont il est régulièrement victime. C'est pourquoi la Maison Blanche avait opéré un revirement sur le chiffrement en expliquant qu'il ne fallait en aucun cas l'affaiblir. Puis avait à nouveau changé d'avis peu après « *l'acte terroriste* » du 2 décembre perpétré à San Bernardino en Californie et revendiqué par l'organisation État islamique.

Au sein même de l'administration Obama, les avis divergent sur la manière d'inciter les entreprises high-tech à coopérer et/ou répondre aux requêtes des forces de l'ordre. La Maison Blanche a refusé de légiférer en ce sens en imposant des *backdoors* aux firmes technologiques et fait depuis des pieds et des mains pour s'attacher la coopération active des géants du web... qui semblent freiner des quatre fers, pris en étau entre la sécurité des données de leurs clients et les impératifs de sécurité nationale qui semblent légitime dans le contexte actuel. Google, Facebook, Snapchat et Whatsapp s'apprêteraient même à accélérer sur le chiffrement en optant pour le *end-to-end* sur l'ensemble de leurs services.

Un juste équilibre est-il possible ? Une solution qui allierait un chiffrement fort, et la possibilité laissée aux autorités d'accéder aux données souhaitées. Le président Obama la appelé de ses vœux et ce, avant que le législateur ne vienne imposer une loi qu'il juge « *dangereuse* ».

La vie privée est une notion très importante chez Jan Koum, le fondateur de Whatsapp, ce dernier ayant grandi sous l'ère soviétique en Ukraine. Il fut l'un des premiers à manifester son soutien à Tim Cook lorsque le CEO d'Apple a publié sa lettre ouverte expliquant les raisons de son opposition au FBI.

« *Notre autonomie et notre liberté sont en jeu* », avait-il alors déclaré sur sa page Facebook.
15 mars 2016

Liens : <http://www.journaldugeek.com/2016/03/15/chiffrement-whatsapp-ligne-mire/>



Uber, Airbnb, Ebay... : la pseudo « économie du partage » planque ses bénéficiaires dans les paradis fiscaux

Encore un article exceptionnel de la part du site Bastamag qui une fois encore nous démontre plus ou moins volontairement que tout n'est que mensonge. Nos gouvernements luttent-ils contre l'évasion fiscale et la fraude? Oui, lorsqu'il s'agit des « petits » comme nous, car ce qu'ils font, cela nous est interdit, et ce qu'ils autorisent à certains, nous n'avons pas le droit de le faire, même très partiellement. Donc au nom de la lutte contre la fraude, le blanchiment d'argent, augmentent les moyens de surveillance, les taxes, mais finalement, rien n'est fait lorsqu'il s'agit de très gros sous, comme rien n'est fait avec le scandale Luxleaks... Et du côté des fraudes, cela continue de plus belle en toute impunité!

L'économie dite « du partage » n'aime pas la répartition des revenus. Encore moins contribuer par l'impôt aux infrastructures des pays au sein desquels elle prospère. Quand il s'agit de fiscalité, les nouveaux acteurs du commerce et des services en ligne, tels Uber, Airbnb, Ebay ou Paypal, suivent la route tracée par les grands frères Google, Apple, Facebook et Amazon : celle du contournement fiscal. Avec la complicité de territoires comme le Luxembourg, le Delaware ou les Bermudes, vers lesquels leurs profits convergent. Les « start-up » françaises les suivent-ils ? A Leetchi ou vente-privee.com, on se défend de toute évasion fiscale. Enquête.

Le service de véhicules avec chauffeurs Uber fait beaucoup parler de lui pour ses conflits avec les taxis et la justice. Le site de location touristique chez les particuliers Airbnb est de son côté en délicatesse avec les hôteliers. Mais, au-delà de la distorsion de concurrence que génèrent ces nouveaux business, savez-vous où part l'argent que vous dépensez quand vous réservez un chauffeur ou quand vous achetez un bien vendu aux enchères en ligne ? Ces nouveaux acteurs de l'économie du net sont moins souvent pointés du doigt pour leur comportement face à l'impôt. Il y a pourtant de quoi. Comme les quatre géants du numérique (Amazon, Apple, Facebook, Google), ces nouvelles entreprises ont la fâcheuse tendance à tout faire pour ne pas payer ce qu'elles doivent à la société.

« Les géants du numérique profitent, comme toutes les entreprises multinationales, des failles des systèmes fiscaux nationaux et des accords bilatéraux pour pratiquer une optimisation fiscale réduisant drastiquement leur taux d'imposition, fait remarquer une note d'analyse sur la fiscalité du numérique du Commissariat général à la stratégie (France stratégie). Avant d'ajouter : « Du fait du caractère immatériel d'une large part de leurs activités et de la difficulté qu'ont les services fiscaux à définir le territoire concerné par les opérations de production, ils parviennent à exploiter ces failles de façon plus importante que les industries "classiques". » C'est tout le problème de l'économie du net. Et ses acteurs en profitent à plein.

Amazon, par exemple, ne paie que 0,5% d'impôt sur son chiffre d'affaires hors des Etats-Unis. La librairie en ligne fait l'objet d'une enquête de la Commission européenne pour les avantages fiscaux dont elle bénéficie grâce à l'implantation de son siège européen au Luxembourg . Et les services fiscaux français lui réclament 250 millions de dollars d'arriérés pour la période 2006-2010. Des procédures similaires sont engagées en Allemagne, au Canada, en Chine, en Inde, au Japon et au Royaume Uni ! . Et les autres font pareil. Hors des Etats-Unis, Google ne paie que 2,2% d'impôt sur son chiffre d'affaires, Facebook 1,5% et Apple 1% . Un modèle que reproduisent les nouvelles stars de la soi-disant « économie du partage »

Avec Airbnb, les profits séjournent en Irlande et au Delaware

Google et Facebook ont leur siège européen en Irlande. Le pays est certes l'un des plus coulant de l'Union européenne en matière de protection des données personnelles. Mais il offre un autre avantage de taille : un taux d'impôt sur les sociétés de seulement 12,5 %, là où il est de 33 % en France. Airbnb les a imité. Le service de location touristique chez des particuliers, qui revendique 40 millions d'utilisateurs, a lui aussi opté pour Dublin pour son siège européen.

Comme l'indiquent ses conditions générales d'utilisation, tous les contrats passés hors des États-Unis se font avec l'entreprise irlandaise, même si Airbnb a une filiale en France, enregistrée à Paris, et une autre en Allemagne, enregistrée à Berlin . Ce contournement fiscal ne s'arrête pas là. Airbnb dispose aussi depuis 2013 de trois filiales à Jersey (Airbnb Limited 1 et 2 et Airbnb International Holding), la petite île anglo-normande qui a figuré jusqu'en 2014 sur la liste des paradis fiscaux du ministère français des Finances.

Au Delaware, plus d'entreprises que d'habitants

La maison mère d'Airbnb, elle, a bien son siège en Californie, à San Francisco. Mais elle est en fait domiciliée à 4800 km de là, dans un minuscule État de la côte Est des États-Unis, le Delaware. Celui-ci compte plus d'entreprises enregistrées – plus d'un million – que d'habitants, environ 930 000 ! L'ONG britannique Tax Justice Network le plaçait il y a encore quelques années à la première place de son classement de l'opacité financière.

Le Delaware, c'est un peu le Luxembourg des États-Unis : un État avec un « *gouvernement favorable aux entreprises* », qui leur offre des conditions d'anonymat et de fiscalité particulièrement avantageuses. « *Le Delaware n'exige pas d'avoir des activités ni mêmes des bureaux situés au Delaware, autre qu'un intermédiaire enregistré. Les propriétaires et les dirigeants ne doivent pas être des citoyens américains. Les dirigeants et investisseurs peuvent voter et prendre des décisions par écrit de n'importe où dans le monde, sans l'obligation de tenir une réunion formelle ; ce consentement écrit peut même être fait par voie électronique* », vante l'État sur son site, en français et dans neuf autres langues, pour attirer les firmes étrangères.

Uber conduit votre argent des Pays-Bas aux Bermudes

Il n'est donc pas étonnant que tant de grandes entreprises du net y aient immatriculé leur siège ou leurs filiales états-uniennes : Amazon, Airbnb, Facebook, sa filiale WhatsApp, Google, Ebay, Netflix . C'est aussi le cas de Spotify (le site de musique) , de l'entreprise française Dailymotion pour sa filiale états-uniennne. Et d'Uber, comme le service de véhicules avec chauffeurs l'indique dans ses conditions générales d'utilisations pour les États-Unis.

L'entreprise qui met en relation chauffeurs et clients a aussi une filiale aux Pays-Bas. C'est d'ailleurs à celle-ci qu'Uber renvoie sur son site en français. En fait, Uber possède au moins sept filiales néerlandaises ! Elles sont toutes enregistrées à la même adresse . Les Néerlandais seraient-ils devenus accros aux voitures avec chauffeurs ? Une autre de ses filiales (Uber International CV), se trouve non pas à Amsterdam mais à Hamilton, la capitale... des Bermudes.

Ebay : des enchères qui passent par les îles Caïmans

Uber International CV, un holding financier, est bien enregistré au Pays-Bas tout en étant en fait immatriculé dans l'archipel listé par la Commission européenne comme un paradis fiscal. Et l'adresse Internet d'Uber International CV indiquée sur l'extrait du registre du commerce des Pays-Bas est bien la même que celle du service de véhicules avec chauffeurs.

Là encore, Uber ne fait que suivre le chemin des plus grands. Google s'était fait épingleur il y a déjà plusieurs années pour ses filiales aux Bermudes qui lui permettaient, grâce à la stratégie dite du « double irlandais », d'échapper aux impôts en transférant ses revenus de filiales en filiales toute en bénéficiant de dispositifs de déduction fiscale. La filiale Google Ireland Holdings est d'ailleurs toujours enregistrée en parallèle en Irlande et aux Bermudes.

Regardons du côté du leader du commerce en ligne Ebay. La liste de ses filiales qui se trouvent dans des pays connus pour leurs avantages fiscaux à de quoi donner le tournis : une dizaine de filiales au Delaware, quatre au Luxembourg dont le siège européen de l'entreprise, deux en Suisse, une à Singapour, et, surtout, deux filiales aux îles Caïmans et une aux îles vierges britanniques. Deux paradis fiscaux notoires.

Paypal : des paiements en ligne via le Luxembourg et Singapour

La même chose vaut pour Paypal, le service de paiement sur Internet qui appartenait à Ebay avant que la multinationale de commerce en ligne ne n'en sépare cette année. Paypal a quatre filiales au Delaware. Son siège européen, plus six autres filiales, se trouvent au Luxembourg. Paypal dispose aussi d'une filiale mixte, implantée à la fois en Irlande et à Singapour, et de deux filiales intégralement singapouriennes. Pourquoi Singapour ? La cité-État asiatique est en bonne place dans le classement de l'opacité financière du réseau Tax Justice Network.

Ebay, Paypal, Netflix, toutes ces entreprises ont choisi, comme Amazon, d'implanter leur siège européen au Luxembourg. À croire que le pays de 500 000 habitants serait le poumon de l'économie européenne et disposerait de plusieurs générations d'informaticiens hors pair. Ces firmes ont pu y être attirées pour le taux de TVA avantageux que le Luxembourg proposait encore jusqu'à cette année : 15% contre 20% en France et au Royaume-Uni, ou 19% en Allemagne. Jusqu'au 1er janvier 2015, un « régime d'exception » permettait aux fournisseurs de prestations électroniques, de l'achat d'un livre (Amazon), d'un bien vendu aux enchères (Ebay) ou d'une série télévisée (Netflix), d'appliquer la TVA du pays vendeur et non du lieu où se trouve l'acheteur. Cette disposition a enfin été annulée.

<http://lesmoutonsenrages.fr/2015/09/21/uber-airbnb-ebay-la-pseudo-economie-du-partage-planque-ses-benefices-dans-les-paradis-fiscaux/>

Quand Facebook et WhatsApp servent à vendre drogues et animaux rare

Plusieurs organisations de défense de la nature sauvage ont déclaré hier que des trafiquants d'animaux publiaient activement leurs offres sur Facebook

Ce cas est loin d'être isolé: depuis plusieurs années le Brésil lutte contre les trafiquants de drogue sur WhatsApp... Mais pourquoi les criminels optent pour ces applications populaires? Et comment les autorités locales combattent ce phénomène? dauphin © Flickr/ Ed Dunens Des pertes importantes de dauphins en Argentine L'organisation Traffic, créée par le Fonds mondial pour la nature (WWF) et l'Union internationale pour la conservation de la nature (UICN), a percé à jour un réseau de trafiquants d'animaux sur Facebook. D'après son dernier rapport en date, les criminels agiraient via des groupes fermés enregistrés en Malaisie occidentale. En se faisant passer pour des acheteurs, les protecteurs des animaux ont rejoint 14 de ces groupes et, en cinq mois, ont relevé plus de 300 annonces de vente d'animaux rares ou en voie d'extinction — des gibbons, des ours malaisiens, des pandas, des tortues et des oiseaux étaient activement achetés en tant qu'animaux domestiques ou pour être revendus. Au total, plus de 100 vendeurs ont été identifiés. un loris © Wikipedia/ Lionel Mauritson un loris Selon Traffic, ces groupes illégaux ont pu voir le jour en Malaisie car dans ce pays, les administrateurs de Facebook ne suivent pas rigoureusement les infractions au règlement du réseau social. En cinq mois d'observation, aucun des groupes n'a été fermé alors qu'ils comptaient presque 68 000 membres. SeaWorld © Flickr/ Josh Hallett SeaWorld reconnaît que ses employés ont infiltré des associations écologistes C'est seulement quand Traffic a fourni les résultats de son investigation à la direction du réseau social pour l'Asie du Sud-Est que l'accès à ces groupes a été immédiatement restreint, et que le personnel de Facebook a promis d'aider les activistes à mettre la main sur les criminels. Tous les documents ont été

transmis aux autorités locales qui ont déjà annoncé l'interpellation de plusieurs dizaines de trafiquants. Néanmoins, les défenseurs des animaux craignent que les ventes d'animaux par le biais des réseaux sociaux soient d'une ampleur bien plus grande. Cependant, toutes ces interdictions ne concernent pas le service de messagerie WhatsApp appartenant à Facebook. Fin 2014, cette application s'est même dotée d'une fonction de cryptage: le message est codé au moment de l'envoi et il ne peut être décrypté que par le destinataire. Une telle approche de la protection des données a suscité l'inquiétude du FBI, dont le directeur a appelé en août 2015 à fournir aux services de renseignement une clé de décryptage — la réponse fut négative. Logo de Facebook © Sputnik. Natalya Seliverstova Le vice-président de Facebook arrêté au Brésil Les autorités brésiliennes sont encore plus révoltées par la politique de WhatsApp, utilisé aujourd'hui par plus de 70 millions d'habitants du pays pour contourner le coût élevé des appels et des SMS. WhatsApp est aussi massivement utilisé pour vendre des armes et des drogues — le Brésil compte officiellement plus d'un million de narcodépendants, dont beaucoup consomment des drogues dures comme le crack et la cocaïne. La police est pratiquement impuissante car WhatsApp refuse de lui fournir l'accès aux correspondances. Cela force le gouvernement brésilien à employer des méthodes peu traditionnelles pour faire pression sur WhatsApp: fin décembre, après un nouveau refus de fournir à la police des informations sur une affaire criminelle, la messagerie a été entièrement bloquée dans le pays pendant 48 heures. Toutefois, cette décision de justice a été levée le lendemain et plus de 1,5 million de Brésiliens ont commencé à utiliser le service protégé Telegram.

<https://fr.sputniknews.com/presse/201603041023121288-vents-drogues-animaux-rares-facebook-whatsapp/>

"Les monnaies virtuelles favorisent le risque d'escroquerie "

Pour Jean-Baptiste Carpentier, directeur de Tracfin, la cellule "anti-blanchiment" de Bercy, les monnaies virtuelles, ainsi que les cartes-prépayées et Monéo présentent un risque.

les monnaies virtuelles, qui s'achètent sur des plates-formes web et servent de moyens de paiement sur certains sites internet, ne sont pas contrôlées par les banques et échappent à la plupart des formes de régulation. Le risque de fraude et de blanchiment, mais aussi d'escroquerie est donc fort", affirme Jean-Baptiste Carpentier. Sipa

Jean-Baptiste Carpentier, directeur de Tracfin, la cellule du ministère de l'Economie qui est en charge du renseignement sur les circuits financiers clandestins, se dit inquiet après le scandale Liberty Reserve. Le 28 mai, la justice américaine a en effet démantelé la plus grande fraude financière jamais décelée sur internet. La société Liberty Reserve est accusée d'avoir blanchi, grâce à sa monnaie virtuelle du même nom, plus de 6 milliards de dollars (4,6 milliards d'euros) en sept ans. Selon Jean-Baptiste Carpentier, la France n'est pas à l'abri de ce type de risque. Il explique pourquoi.

Après le scandale Liberty Reserve aux Etats-Unis, craignez-vous que l'utilisation de monnaie virtuelle favorise le blanchiment d'argent ?

Oui. Je ne suis d'ailleurs pas du tout surpris par ce scandale, mais inquiet qu'une affaire semblable se produise en France. Car les monnaies virtuelles, qui s'achètent sur des plates-formes web et servent de moyens de paiement sur certains sites internet, ne sont pas contrôlées par les banques et échappent à la plupart des formes de régulation. Le risque de fraude et de blanchiment, mais aussi d'escroquerie est donc fort. En revanche, il convient de souligner que la monnaie électronique, c'est-à-dire les cartes prépayées ou le système Monéo, fait l'objet d'une régulation, issue de directives européennes et d'une loi française. Ces instruments sont légaux lorsqu'ils respectent cette régulation. Mais cette devise électronique constitue néanmoins un instrument à risque dans la mesure où elle favorise l'anonymat : en

pratique, ces cartes peuvent devenir des « comptes au porteur », dont on ne connaît pas l'identité du détenteur. Or ces comptes ont justement été supprimés en France et à l'étranger, dans le cadre de la lutte anti-blanchiment. Sauf à limiter strictement l'emploi de ces cartes à des montants minimes, leur usage est donc largement contradictoire avec les mesures mises en œuvre en ce domaine depuis plus de vingt ans.

Comment fonctionne le schéma de blanchiment par de la monnaie virtuelle ?

Je peux obtenir de la monnaie virtuelle, la liberty reserve par exemple, en l'achetant sur internet, souvent à l'étranger, via ma carte bancaire ou tout autre moyen de paiement. Ensuite j'achète n'importe quels produits, de la drogue ou des armes, que je paye avec cette monnaie virtuelle. L'argent est ainsi blanchi. Il est difficile de tracer les opérations, qui ne sont surveillées par personne.

Combien de cas avez-vous déjà repéré en France ?

Tracfin a déjà détecté plusieurs cas. Nous en avons transmis certains à la justice, ces affaires sont en cours d'enquête.

Peut-on imaginer en France des affaires de l'ampleur de celle des Etats-Unis ?

En principe non, les montants ne seront pas les mêmes, le marché n'a pas la même taille. Et les Français sont moins sensibles à ces nouveaux moyens de paiement, car l'économie est très bancarisée. La plupart des habitants possèdent un compte, contrairement à beaucoup d'autres pays. Nous sommes probablement moins exposés aux risques que les Américains.

Quel est le volume ou le montant des monnaies virtuelles et électroniques ?

Je n'avancerai aucun chiffre. C'est comme les données sur la délinquance, c'est très difficile à estimer. Mais les monnaies virtuelles et électroniques semblent être beaucoup plus développées à l'étranger, notamment en Russie ou aux Etats-Unis. Quoiqu'il en soit, c'est un sujet amené à prendre de l'ampleur. Dès 2011, Tracfin a tiré la sonnette d'alarme en France et auprès de la Commission européenne, qui avait adopté une logique très libérale sur la question. Notre rapport annuel indiquait clairement notre préoccupation sur les monnaies virtuelles et sur certains risques liés à la monnaie électronique. Je pense qu'on a laissé naître un système intrinsèquement dangereux.

Vous déconseillez aux Français l'usage de monnaie virtuelle, qui permet par exemple de diminuer les frais lors de l'envoi d'argent d'un pays à l'autre ?

Je n'ai pas à donner de conseil, mais l'affaire autour de la monnaie liberty reserve et les évolutions erratiques de la monnaie virtuelle la plus connue, le bitcoin, incitent à la prudence. Voir son compte saisi, parce qu'on ne savait pas qu'il y avait le FBI derrière, ou sa valeur diminuer en quelques heures n'est pas très rassurant ! Par ailleurs, l'opacité de beaucoup de ces monnaies peut favoriser des escroqueries au détriment du consommateur. Personnellement, je souhaite que les monnaies virtuelles soit régulées, voire interdites pour certaines d'entre elles.

<http://www.challenges.fr/economie/20130603.CHA0244/les-monnaies-virtuelles-favorisent-le-risque-d-escroquerie.html>

Blanchiment d'argent sur eBay avec de faux scooters

Eric Vernier est docteur en sciences de gestion et maître de conférences. Il a écrit « Techniques de blanchiment et moyens de lutte », paru aux éditions Dunod. Entretien.

Quels types de trafics trouve-t-on sur les sites de vente d'occasion ?

Il y a quatre grands axes : l'escroquerie, la contrefaçon, le recel et le blanchiment d'argent. Il y a quelques années, le recel se pratiquait « au cul du camion », maintenant c'est « au cul » de

ces sites. On y retrouve indifféremment de la petite escroquerie, des bandes organisées comme des organisations criminelles.

Comment se déroule le blanchiment d'argent ?

Le blanchiment peut se faire grâce à la vente de produits inexistant entre complices. Je me souviens de cette histoire de scooters de collection, vendus à des prix largement supérieurs au cours du marché.

C'est l'un de vos collègues, lui même collectionneur, qui m'avait alerté. Il s'étonnait du prix affiché dans certaines annonces diffusées sur eBay, supérieur de 30% à 50% à la cote officielle.

En y regardant de plus près, l'astuce, c'était de les vendre le plus cher possible, afin d'obtenir la trace de transactions et justifier des transferts d'argent. Vendeurs et acheteurs appartiennent en fait à la même organisation.

Les vérifications vont être difficiles à effectuer. Je me suis rendu compte de la manipulation lorsque j'ai téléphoné aux numéros affichés dans ces annonces. Soit ce numéro était erroné, soit le scooter en question était vendu. Ce devait être un réseau assez important, pour que ce soit aussi visible.

Mais le blanchiment peut s'effectuer grâce à l'achat de produits existants, payés avec de l'argent sale.

Dans les deux cas, ces ventes justifient des rentrées d'argent officielles en cas de contrôle par la police ou le fisc. Ce blanchiment est pratiqué par des amateurs, mais aussi par des organisations « professionnelles », en d'autres proportions.

Que peuvent faire les autorités face à ces trafics ?

On est dans le domaine du virtuel, donc le contrôle est difficile. Il y a une atomisation des échanges. Dans une boutique mondiale sur la Toile, la police comme la justice ne peuvent pas faire grand chose.

De temps en temps, ils arrêtent un réseau, mais c'est vraiment pour l'exemple. Les autorités forcent les sites à mettre en place des procédures de contrôle. Ces derniers s'exécutent, mais les outils qu'ils créent sont peu efficaces. Au final, tout le monde est content, et le blanchiment continue...

Je ne vois a priori aucune possibilité de contrôle sur ce type de délits. Comment voulez-vous évaluer la contrefaçon, puisque la photo de l'annonce est généralement authentique ?

<http://rue89.nouvelobs.com/rue89-eco/2012/03/05/comment-blanchir-largent-ebay-faux-scooters-228777>

Les jeux sur Internet favorisent le blanchiment

Dans un rapport, le service central de prévention de la corruption affirme que «le grand banditisme a su tirer profit de l'économie virtuelle», et met en garde l'État sur les risques d'Internet.

Côté statistiques, l'état de la corruption en France n'a pas bougé. Le nombre de jugements prononcés depuis dix ans est quasiment stable : en 2006, une centaine de chefs d'entreprise, élus ou fonctionnaires ont été définitivement condamnés pour corruption active ou passive, pour des scandales remontant souvent à plusieurs années. Le dernier rapport du service central de prévention de la corruption (SCPC), dont Le Figaro a pris connaissance, relève même que ce genre de dossiers ne représente que 0,023 % des «affaires poursuivables» dans les tribunaux de la région parisienne. «Des progrès en terme de détection paraissent envisageables», estime sobrement le magistrat Michel Barrau, chef de cet organisme interministériel créé en 1993 et qui dépend du garde des Sceaux.

Le service central de prévention de la corruption adresse cette année sa principale mise en garde aux partisans de la libéralisation des jeux sur Internet. Nouvelles formes de fraudes, enquêtes rendues presque impossible par la multiplicité des interlocuteurs... Selon le rapport du SCPC, l'ampleur actuelle des flux suspects est de nature à multiplier les délits de corruption et de blanchiment. Pour la criminalité organisée, décrit le rapport, «il est relativement facile de blanchir des fonds illégaux à partir d'un site de jeu sur Internet». Les casinos virtuels, souvent basés à Malte ou à Gibraltar pour des raisons fiscales, permettent, par exemple, de fournir des gains de jeu officiels à des joueurs ayant misé de l'argent sale. Il s'agit simplement de la version moderne du blanchiment ou du casino utilisé jadis par les mafias italiennes ou new-yorkaises.

Autre grand risque de ces salles de jeu apparues sur Internet : les nouvelles corruptions autour des compétitions sportives. Il s'agit pour un groupe criminel de corrompre joueurs ou entraîneurs afin de truquer les matchs sur lesquels des millions d'euros sont pariés. Le rapport relève que les autorités mondiales du football sont déjà vigilantes sur l'activité des bookmakers, mais «il serait souhaitable que les lobbyistes et les États qui prônent l'ouverture à la concurrence de ce secteur prennent conscience qu'il ne s'agit pas d'une activité économique ordinaire mais d'un secteur dans lequel le risque est patent, connu, irréfutable et que le choix de l'absence de contrôle pourrait favoriser la criminalité.»

L'obstacle du secret bancaire

Faisant allusion à l'affaire du cercle Concorde, cercle de jeu parisien fermé il y a tout juste un an avant une série de mise en examen pour association de malfaiteurs, extorsion de fonds et corruption, le rapport du SCPC insiste : «des exemples récents montrent qu'il est difficile de contrôler des jeux installés physiquement sur un territoire. Qu'en sera-il alors, si on y ajoute l'utilisation d'Internet et des paradis fiscaux ?» Sur ce point, la lutte contre les mafias ayant trouvé des débouchés sur les casinos virtuels et les longues enquêtes financières internationales se rejoignent. Elles butent sur les mêmes barrages. Les investigations se heurtent systématiquement à la difficulté de retracer les flux financiers empruntés.

Le juge financier Renaud Van Ruymbeke, intervenant récemment au cours d'un colloque organisé par la société d'avocats Carbonnier Lamaze Rasle, exposait ainsi que «face aux détournements menés par le biais de circuits offshore, il faudrait s'interroger sur des mesures comme la levée du secret bancaire en Suisse, au Liechtenstein, à Gibraltar ou aux îles Caiman, mais on se heurte à des résistances très fortes» .

<http://www.lefigaro.fr/actualite-france/2008/11/10/01016-20081110ARTFIG00581-les-jeux-sur-internet-favorisent-le-blanchiment-.php>

Arnaque Western Union : Les différents scénarios possibles

L'arnaque Western Union ainsi que d'autres arnaques de ce type et provenant de Côte d'Ivoire sont très nombreuses, et même en augmentation ces derniers mois. Si vous avez déjà vécu ce genre d'arnaques, vous aviez probablement eu affaire à l'une citées dans cet article.

L'arnaque au client mystère (Secret Shopper)

Vous êtes contacté soudainement (souvent en anglais ou dans un français catastrophique) par un individu qui vous propose de faire une mission en tant que « client mystère ». Vous recevez des « *traveller chèques* » (chèques de voyage) d'un montant important avoisinant généralement le millier d'euros et quelques semaines plus tard, vous apprenez qu'ils ont été refusés par votre banque car ils ont été contrefaits ou volés.

Entre temps, vous avez bien entendu reversé une rémunération de quelques centaines d'euros et viré le montant restant à une personne X ou Y. Ce montant, vous ne le reverrez jamais en plus de ne pas recevoir votre rémunération... Dans ce cas là, il est primordial de prendre

contact avec la société émettrice des voyageurs chèques afin de vérifier le numéro de série, cela prend 5 minutes et vous pourrez les jeter à la poubelle directement sans vous faire arnaquer.

L'arnaque aux sentiments

Les cyber-escrocs créent des faux comptes sur des sites de rencontre, ou sur les réseaux sociaux en utilisant des photos d'hommes ou de femmes récupérées sur internet. Leur but est d'entretenir pendant des semaines voir des mois des conversations sentimentales avec des internautes.

Les cibles sont souvent choisies, c'est-à-dire des personnes qui sont déjà affaiblies sentimentalement au moment de la rencontre. À un moment donné, ils solliciteront leur victime pour l'achat d'un billet d'avion leur permettant de leur rendre visite, pour l'achat de quelques nuitées à l'hôtel, pour aider un proche tombé soudainement malade ou victime d'un accident, etc. Les raisons ne manquent pas, les seules limites sont la capacité d'imagination de l'escroc !

Ces arnaqueurs qui se font appeler « *brouteurs* » en Côte d'Ivoire maîtrisent très bien la langue française ainsi que les outils informatiques, dont les logiciels webcam truqués et de retouches d'images. Les excuses données par la suite sont très banales, on apprend qu'ils se sont fait arrêter à l'aéroport car leurs vaccinations n'étaient pas à jour, ou car un autre phénomène « imprévisible » est arrivé. Dans ce cas, il n'y a que la vivacité d'esprit et la perspicacité qui peut empêcher de tomber dans le panneau. Ne pas être trop crédule, surtout sur le Net avec des total inconnus.

L'arnaque à l'héritage

Il s'agit en général de prétendus fonds (des dizaines de milliers d'euros) qui se trouveraient bloqués dans une certaine banque au nom d'un certain héritier ne pouvant récupérer son avoir sans l'intervention d'un tiers. Les escrocs manient là encore très bien la langue française et font douter les internautes en utilisant des noms réels et des adresses mail qui semblent légitimes.

Les escrocs récupèrent ensuite vos coordonnées bancaires ou vous font payer plusieurs « frais de dossier » ou douaniers en cascade. Les motifs donnés sont très variés, il peut s'agir d'une personne atteinte d'une grave maladie ou décédée, d'un objet qui n'a pas pu être livré, etc. Avec une simple recherche Google sur le mail de l'escroc, vous tombez généralement sur des résultats probants.

Les arnaques Le Bon Coin

Ces arnaques prennent plusieurs formes mais ont habituellement toutes un point commun : une offre excessivement alléchante. Certains escrocs répondent à vos annonces en indiquant être un acheteur résidant en Côte d'Ivoire. Ils demandent l'expédition de votre objet (souvent de véhicules) depuis la France à vos frais avec promesse de règlement dès réception, ou en demandant vos coordonnées bancaires pour un prétendu « paiement ».

D'autres escrocs vendaient sur Le Bon Coin des objets en demandant un paiement par mandat-cash, bien-sûr les acheteurs ne recevaient jamais leur commande. Faites également attention avec votre numéro de téléphone, lorsque vous initiez une conversation de ce type, vous risquez d'être inondé d'appels et de SMS toute la journée !

L'arnaque à la loterie

L'une des plus populaires, et sûrement l'une des moins efficaces à présent. Les mails finissent en grande majorité dans les dossiers spam et ne sont pas convaincants. L'un des derniers en date était plutôt marrant, à savoir une "Loterie Microsoft" accompagnée de photos de Bill Gates, vous annonçant que vous êtes l'heureux gagnant de plusieurs dizaines de milliers d'euros. Fake !

L'arnaque Skype (anciennement MSN)

Votre contact réel se fait pirater et l'escroc se sert du compte pour demander de l'aide, notamment pour l'achat d'un objet ou le paiement d'un loyer.

L'arnaque au remboursement

Pour vous faire croire que l'on va vous aider, on vous propose des faux sites et fausses adresses mail à contacter, tout en cherchant à vous arnaquer une deuxième fois.

Ne croyez absolument pas les sites qui vous proposent de vous aider ou de vous rembourser, pareil pour les adresses mail du type « *interpole-service-anti-arnaque@hotmail.etc* ». A noter qu'il y a eu plusieurs commentaires de ce type postés sur UnderNews depuis un an, la plupart modérés.

Les seules vraies adresses et sites se trouvent à la fin de cet article.

D'autres arnaques plus techniques

Le phishing ou hameçonnage, vous recevez un mail provenant soi-disant de *PayPal* ou de votre banque vous demandant de mettre à jour vos informations. Plus dangereux encore, un faux mail de paiement PayPal en réponse à la vente d'un objet en ligne sur un site de petites annonces : vous envoyez alors l'objet en pensant avoir été payé mais il n'en ai rien ! Pensez à vérifier systématiquement dans votre compte PayPal que la somme a bien été véritablement versée (ne surtout pas accorder de l'importance aux mails reçus).

Cette arnaque est très utilisée sur Le Bon Coin ou eBay et fait énormément de victimes en France. Un reportage au journal de 20H a d'ailleurs été diffusé juste après les fêtes pour avertir des risques.

Et le pire dans tout ça ?

Beaucoup de victimes arnaquées ne portent pas plainte, car elles se sentent embarrassées d'être tombées dans le piège.

Celles qui portent plainte ne revoient tout de même pas leur argent ou objet car la police française ne prend pas souvent (jamais ?) le temps de faire les démarches. Les escrocs se trouvent à l'étranger et sont, pour la plupart du temps, intouchables.

Comment éviter ces arnaques ?

Ne faites d'une manière générale absolument pas confiance aux annonces de ce type, et restez vigilant et informés. Ne répondez pas aux mails lorsqu'ils sont alléchants ou vous demandent vos identifiants et/ou informations bancaires.

Utilisez TinEye sur les images des réseaux sociaux et annonces pour savoir si l'image a été récupérée sur Internet ou non.

Comment récupérer votre argent ?

Telle est la question. L'arnaque western union (ou toute autre arnaque de ce type) est compliquée à traiter pour les autorités.

Vous pouvez bien-sûr déposer plainte en France, ce qui est d'ailleurs le seul choix possible pour que vous puissiez obtenir une réponse favorable, à condition que la justice française décide de poursuivre son enquête en Côte d'Ivoire, le consulat transmettra alors la commission rogatoire internationale aux autorités ivoiriennes.

Si vous déposez plainte en Côte d'Ivoire, vous vous exposez à des frais de déplacement élevés, alors que la probabilité de récupérer vos fonds reste toujours extrêmement faible, pour ne pas dire nulle.

<http://www.undernews.fr/reseau-securite/arnaque-western-union-les-differents-scenarios-possibles.html>

Vous attrapez des Pokemons ? PokemonGO attrape votre vie 2.0

La folie estivale autour du jeu PokemonGo a laissé les observateurs du numérique dubitatifs. Si le jeu est très sympathique, aviez-vous vu que Pokemon Go cartographiait votre vie numérique ?

C'est le blog Data Security Breach qui en parle dans ses colonnes. PokemonGo est un jeu sympathique mais à l'appétit féroce dès qu'il s'agit de vos données. Il suffit de marcher dans les rues, dans les parcs, sur les plages pour croiser des centaines de « dompteurs » et comprendre que le big data se fait à leur détriment. DataSecurityBreach.fr se pose la question à savoir si ce jeu n'est qu'un maître espion, capable de cartographier les informations que les Google Cars, par exemple, n'ont plus « flasher ». Data Security Breach référence dans son article « *PokemonGo : un ami qui vous veut du mal* » toutes les « infos » que réceptionnent l'application. Certaines pourraient même laisser penser à un espionnage pur et dur de l'utilisateur. Bref, PokemonGo rappelle que si un produit est gratuit, c'est l'utilisateur qui en fera les frais.

Je vous relatais, dernièrement la folie des fausses applications Pokemon avec de vrais morceaux de codes malveillants ; ou encore les attaques numériques qu'ont subit les serveurs du jeu par des pirates informatiques adeptes de DDoS et en mal de gloire. A noter une sacré business, aussi, pour certains pirates et des outils de triche qui permettent de passer d'une localisation GPS à une autre, pour récupérer les personnages du jeu, sans bouger de son canapé. Certains n'hésitent pas à montrer leur « méthode » sur des chaînes Twitch !

<http://www.zataz.com/attrapez-pokemons-pokemon-attrape-vie-2-0/#axzz4L4o2Pce5>

Un code malveillant dans un système de lecture de CB

Le groupe de restaurant Pizza & Pub Village informe ses clients d'une attaque informatique. Un code malveillant a été injecté dans des lecteurs de cartes bancaires (POS).

Le site DataSecurityBreach révèle un piratage informatique particulièrement intéressant. Le groupe de restauration Village Pizza & Pub vient d'informer ses clients d'une intrusion dans son système informatique. Un logiciel espion a été introduit dans le système de paiement par carte bancaire des restaurants. Un cheval de Troie installé à partir de l'outil de TransformPOS, un fabricant de lecteurs de CB. TransformPOS a assuré que la cause de l'incident avait été identifiée et résolue.

Pendant ce temps, en France...

L'Observatoire national de la délinquance et des réponses pénales (ONDRP) a indiqué que plus de 800.000 ménages Français se sont déclarés victimes d'une escroquerie bancaire en 4 ans. Un chiffre tiré de plaintes, entre 2011 et 2014. D'après cette étude, 35% des escroqueries sont inférieures ou égal à 100 €. 25%, entre 301 et 1000 €. 17% sont supérieures à 1000€. Près de 8 ménages escroqués sur 10 ont été remboursés. 12% de l'argent volé est récupéré par le pirate via un distributeur de billets (donc du skimming qui a permis de cloner la carte, NDR). 60% est récupéré via un achat direct sur la toile. 17 % des cas, le pirate a recours à un autre type de blanchiment. Les cas sont multiples, ZATAZ.COM a déjà pu repérer des rechargements de crédit téléphoniques ; des placements dans des casinos douteux ; des achats de comptes sur des sites pornographiques qui sont revendus... Une étude très (trop) généraliste pour que le publique comprenne véritablement le danger, les possibilités de fuites et comment véritablement se protéger.

Comment se protéger ?

Votre carte bancaire ne doit jamais quitter votre regard lors d'un achat en boutique, un paiement dans un restaurant. Protégez votre carte dans un étui qui empêchera l'interception NFC sans votre accord. Retournez TOUJOURS le lecteur de carte bancaire qui vous est présenté par un commerçant. Est-ce que les visses ont été abimées ? Y-a-t-il un autocollant qui protège le boîtier, nous avons eu des cas où les commerçants s'étaient fait subtiliser leur lecteur de CB, remplacé par une version pirate. Sur Internet, bannissez l'utilisation de votre vraie CB. Demandez à votre banque le moyen qu'elle a mis pour vous permettre de générer une carte bancaire unique, pour un achat, un montant. Le Crédit Mutuel du Nord, par exemple, propose la *PayWeb Card*. Votre commerçant est payé, et si par on ne sait quel hasard il se fait voler le numéro de carte bancaire que vous avez fourni, le pirate ne pourra rien en faire et votre argent est protégé.

Dernier détail, ne perdez jamais du regard votre téléphone portable. Le clonage de votre puce peut permettre à un pirate de valider des achats via un SMS de validation de votre banque en se faisant passer pour votre téléphone.

Bref, n'oubliez jamais que pour les pirates informatiques nous ne sommes que des portes monnaie sur pattes et qu'ils ne manquent pas d'imagination pour mettre la main sur des données bancaires.

<http://www.zataz.com/un-code-malveillant-dans-un-systeme-de-lecture-de-cb/#axzz4A3JYqryt>

2 millions de dollars dérobés via des skimmers Bluetooth implantés dans des stations services aux USA

Les cybercriminels exploitent toutes les technologies pour faire de l'argent et le Bluetooth ne semble pas être épargné. Un énorme vol de cartes de crédit dans des stations services US a été commis via des skimmers Bluetooth.

13 hommes sont soupçonnés et accusés d'avoir dérobés des milliers d'informations bancaires, en utilisant des skimmers Bluetooth implantés dans des stations service dans le sud des États-Unis. Les informations de cartes de crédit volées leur auraient permis de récupérer plus de 2 millions de dollars via les ATM (les codes PIN des clients ont été aussi enregistrés et l'argent était retiré en cash à des distributeurs automatiques de billets à Manhattan).

Les dispositifs de skimming ont été installés à l'intérieur des machines, de façon indétectable aux gens qui ont payé aux pompes automatiques et les appareils étaient équipés en Bluetooth, de sorte qu'il n'y a pas besoin d'un accès physique pour récupérer les données volées.

Entre mars 2012 et mars 2013, les suspects ont utilisé des fausses cartes bancaires ré-encodées pour retirer de l'argent à partir de distributeurs automatiques de billets, puis déposés l'argent volé dans divers comptes bancaires à New York, en Californie ou encore au Nevada. Une énorme affaire de fraude bancaire en somme...

« Chacune des transactions était moins d'un montant de \$10 000. Elles auraient été structurées de manière à éviter toutes les exigences de déclaration des transactions en espèces imposées par la loi et à déguiser la nature, la propriété et le contrôle des produits de la criminalité des accusés. Du 26 mars 2012, à 28 mars 2013, les cybercriminels sont accusés du blanchiment d'environ 2,1 millions de dollars ».

Les quatre principaux accusés sur les 13 – Garegin Spasrtalyan, 40 ans, Aram Martirosian, 34 ans, Hayk Dzhandzhapanyan, 40 ans, et Davit Kudugulyan, 42 ans – sont considérés comme les organisateurs et sont accusés de vol, de blanchiment d'argent et de la possession d'instruments de falsification et de contrefaçon. Les autres criminels sont chargés de deux chefs d'accusation : vol et blanchiment d'argent.

Ils risquent tous plusieurs années de prison ferme et de gros dédommagements... affaire à suivre.

<https://www.undernews.fr/hacking-hactivisme/2-millions-de-dollars-derobes-via-des-skimmers-bluetooth-implantes-dans-des-stations-services-aux-usa.html>

Etats-Unis: un site de monnaie virtuelle démantelé pour blanchiment d'argent

La justice américaine a mis fin au site de monnaie virtuelle Liberty Reserve, un service utilisé par un million de personnes. Ce serait l'une des plus grosses plateformes de blanchiment d'argent démantelée au monde.

Mardi 28 mai, la justice américaine a affirmé avoir mis fin à ce qu'elle appelle la plus grosse opération de blanchiment d'argent du monde, effectuée par l'intermédiaire de Liberty Reserve, un site internet de monnaie numérique virtuelle. Il aurait permis le blanchiment de six milliards de dollars, soit près de cinq milliards d'euros.

Transformer des dollars en argent virtuel sans contrôle

Sur Liberty Reserve, les internautes pouvaient déposer les sommes qu'ils voulaient anonymement, et de nombreux criminels en ont profité. Le système était simple: il suffisait de s'inscrire en donnant juste un nom que personne ne vérifie. En clair, un faux nom.

Les utilisateurs pouvaient ensuite envoyer 10.000 dollars bien réels qui seront convertis en monnaie numérique. Avec cette monnaie numérique, ils pouvaient acheter n'importe quoi, pour le revendre ensuite et racheter à nouveau. Une fois le business fini, les internautes n'avaient plus qu'à reconvertir leur monnaie numérique en dollars sonnants et trébuchants.

Un million d'utilisateurs, cinq milliards d'euros

Pour la justice américaine, le blanchiment d'argent criminel était le fonds de commerce de Liberty Reserve, issu de la fraude à la carte bancaire jusqu'à la pornographie infantile, en passant par le piratage informatique. Un million de personnes utilisaient ce site dans le monde dont 200.000 aux Etats-Unis.

Les sites de monnaie numérique, comme le Bitcoin, remportent un succès grandissant et le gouvernement américain précise qu'il ne s'oppose pas à toute forme d'argent virtuel. Mais il explique que le risque de blanchiment est toujours élevé et que l'impunité et l'anonymat, même sur Internet, ont leurs limites.

<http://bfmbusiness.bfmtv.com/entreprise/etats-unis-un-site-monnaie-virtuelle-demantele-blanchiment-d-argent-525010.html>

Coup dur pour la finance participative : 900 000 épargnants floués !

Une plateforme de prêts participatifs (crowdfunding) engloutit 7 milliards d'euros et ruine 900 000 épargnants, ça se passe en Chine, mais c'est un avertissement des risques pesant sur ce segment de la finance grise (shadow banking). Explications de Deontofi.com

Une plateforme de prêts participatifs entre particuliers et entreprises frauduleuses ruine 900 000 épargnants en escroquant 7 milliards d'euros, ça se passe en Chine, mais ne croyez pas que cela n'arrive qu'aux autres. La faillite de la start-up de crowdfunding Ezubao est un avertissement des risques pesant sur ce segment de la finance grise (shadow banking). Explications de Deontofi.com

Se passer des banques qui ne font pas leur travail de financement de l'économie, en mettant directement en relation les épargnants et les emprunteurs, ou les entreprises en manque de capitaux. C'est la belle idée du crowdfunding, le financement participatif, ou financement par la foule, rendue possible par l'explosion des réseaux sociaux et l'émergence de l'internet collaboratif. Mieux qu'un financement bancaire, le financement participatif rendrait tout le monde heureux : les emprunteurs ayant accès à des crédits moins coûteux et surtout moins contraignants en terme de démarches, justificatifs, sélection et garanties de remboursement; les particuliers obtenant une meilleure rentabilité de leur épargne en la mettant au service de l'économie réelle, le tout simplement grâce à ces plateformes dont la petite commission est bien inférieure à la marge d'intérêt et aux frais dont se gavent les banques.

Plus besoin de banques ! L'idée est séduisante et bénéficie d'un capital de sympathie indiscutable vis-à-vis du public enthousiaste. Qu'on en juge : 1,5 million de Français auraient prêté 85,2 millions d'euros, investi 24,3 millions d'euros ou soutenu un projet avec 23,7 millions d'euros de dons (dont 20 millions « avec récompense » c'est-à-dire contre un produit ou service), dans le cadre d'opérations de crowdfunding au premier semestre 2015, soit deux fois plus qu'au premier semestre 2014, selon le dernier baromètre de l'association Financement Participatif France.

Il faut dire que le financement participatif, qui était longtemps hors-la-loi au regard des réglementations financières, a bénéficié d'une réglementation allégée légalisant et facilitant son développement, comme Deontofi.com l'avait évoqué dès 2014.

« En France, l'ordonnance du 30 Mai 2014 et le décret du 16 septembre 2014 relatifs au financement participatif ont régulé le secteur du prêt et de l'investissement participatifs en instaurant deux statuts spécifiques (intermédiaire en financement participatif pour le prêt et conseiller en investissements participatifs pour l'investissement) qui permettent aux plateformes respectant la législation de bénéficier d'un label. Le gouvernement a ainsi à plusieurs reprises affiché sa volonté de faire de la France le pays leader du crowdfunding, qui rencontre en effet particulièrement de succès dans l'Hexagone », explique ainsi le ministère de l'écologie, du développement durable et de l'énergie sur son site Internet.

Difficile dans ces conditions de mettre en garde les épargnants contre les risques d'arnaques au crowdfunding, sans passer pour un ringard réac défendant le pré-carré des banques. Les lecteurs de Deontofi.com savent bien que ce site d'information n'est pas complaisant avec les lobbies bancaires.

Le problème est que le crowdfunding, sous son visage sympathique, est aussi un boulevard facilitant l'accès de nombreux escrocs à l'épargne publique. Il suffit de s'inventer un projet écolo, ou techno, ou d'entrepreneuriat social dans la tendance du moment, ou au contraire miser sur l'appât du gain avec un mirage immobilier ou n'importe quel château en Espagne, pour convaincre les épargnants confiants de donner leurs économies en échange d'une promesse de rendement élevé pour couronner le tout.

La recette est d'une banalité aussi affligeante qu'efficace, car c'est bien la même qui a permis à la plateforme de financement participatif chinoise Ezubao de collecter 7 milliards d'euros auprès de 900 000 épargnants, en leur promettant des taux d'intérêt entre 9% et 14,5% sur des prêts à d'improbables entreprises fictives.

Près d'un million d'épargnants ne reverront jamais leur argent

L'arrestation du fondateur d'Ezubao, le jeune Ding Ning (34 ans) et d'une vingtaine de ses employés, à Pékin dimanche 29 janvier 2016, a révélé au monde que tout était faux. La start-up était devenue leader chinois du financement participatif en dix-huit mois, à grand renfort de publicités, en engloutissant l'épargne de ses derniers pigeons pour entretenir l'illusion de rentabilité promise aux pigeons précédents dont le capital ne serait jamais remboursable. Quand cette spirale n'a plus trouvé assez de pigeons pour s'entretenir, elle s'est écroulée.

C'est ce qu'on appelle un système d'épargne pyramidal, ou encore système de Ponzi, redevenu célèbre au XXIème Siècle grâce aux prouesses de Bernard Madoff, incontestable recordman de l'escroquerie pyramidale.

Encore une fois, Deontofi.com n'est évidemment pas opposé aux vertus du crowdfunding. D'ailleurs, qui peut l'être ? Mais notre devoir est de mettre en garde les épargnants sur les risques de déceptions liées aux espoirs qu'ils fondent sur le financement participatif, car beaucoup ne reverront jamais leur argent ni même les intérêts ou formidables gains promis.

<https://deontofi.com/coup-dur-pour-la-finance-participative-900-000-epargnants-floues/>

Pégase, le cheval ailé qui vole (les épargnants) et s'évapore avec leur argent !

Alors que le gendarme boursier alerte les épargnants sur le retrait d'agrément d'un escroc régulé du trading Forex, les sites de ce courtier chypriote, le bien nommé Pegase Capital Ltd, se sont évaporés avec l'argent des clients.

Le gendarme boursier alerte les épargnants qu'une poignée de sites de trading appartenant au courtier chypriote Pegase Capital Ltd mettent la clé sous la porte. Prise en flagrant délit de tromperie, ce voleur chypriote séduisait les épargnants français en revendiquant son caractère régulé, avec un agrément. Mais son comportement n'avait rien d'un courtier régulé. Ses activités n'étaient absolument pas conformes à l'agrément qu'il affichait pour mieux tromper les épargnants. Le gendarme boursier chypriote, la Cysec, avait donc « suspendu » l'agrément de Pegase Capital depuis le 4 mars 2016, dans l'attente des améliorations nécessaires pour mériter réellement cet agrément. Illusoire, bien sûr !

Un escroc ayant pris un déguisement d'intermédiaire régulé n'a ni l'envie ni la capacité à se mettre en conformité avec les règles, car elles sont incompatibles avec son modèle d'enrichissement basé sur le détournement d'argent.

Sentant le vent tourner, Pegase Capital a préféré abandonner définitivement son statut d'escroc régulé, en renonçant à son fameux agrément chypriote...

Résultat, le cheval ailé s'est envolé, car Pegase sait très bien voler. Il suffit de lire la mythologie grecque pour comprendre qu'il a volé et trompé les mortels épargnants impressionnés par son agrément de voleur régulé, pour rejoindre Zeus qui l'a transformé en constellation d'étoile.

En clair, les épargnants qui sont invités à retirer leur argent n'ont probablement guère de chance de revoir la moindre poussière de centime de leurs économies. Les sites internet de trading litigieux ont déjà disparu du cyber-espace, et l'AMF n'est même pas sûr que l'écurie dudit cheval volant soit encore à la même adresse.

L'argent placé chez cet escroc régulé s'est probablement aussi évaporé dans les étoiles, sur les ailes de Pégase qui l'a volé.

Le conseil de Deontofi.com : **NE PLACEZ JAMAIS D'ARGENT CHEZ UN COURTIER CHYPRIOTE** !

Les sites de trading « régulés » sont des escroqueries régulées. Vous avez la garantie de perdre votre argent.

ATTENTION : cette opinion est valable aussi pour les sites de trading sponsors des clubs de foot !!! Vous ne reverrez jamais l'argent que vous leur confiez.

<https://deontofi.com/pegase-le-cheval-aile-qui-vole-les-epargnants-et-sevapore-dans-les-etoiles/>

Coup dur pour la finance participative : 900 000 épargnants floués !

Une plateforme de prêts participatifs (crowdfunding) engloutit 7 milliards d'euros et ruine 900 000 épargnants, ça se passe en Chine, mais c'est un avertissement des risques pesant sur ce segment de la finance grise (shadow banking). Explications de Deontofi.com

Une plateforme de prêts participatifs entre particuliers et entreprises frauduleuses ruine 900 000 épargnants en escroquant 7 milliards d'euros, ça se passe en Chine, mais ne croyez pas que cela n'arrive qu'aux autres. La faillite de la start-up de crowdfunding Ezubao est un avertissement des risques pesant sur ce segment de la finance grise (shadow banking). Explications de Deontofi.com

Se passer des banques qui ne font pas leur travail de financement de l'économie, en mettant directement en relation les épargnants et les emprunteurs, ou les entreprises en manque de capitaux. C'est la belle idée du crowdfunding, le financement participatif, ou financement par la foule, rendue possible par l'explosion des réseaux sociaux et l'émergence de l'internet collaboratif. Mieux qu'un financement bancaire, le financement participatif rendrait tout le monde heureux : les emprunteurs ayant accès à des crédits moins coûteux et surtout moins contraignants en terme de démarches, justificatifs, sélection et garanties de remboursement; les particuliers obtenant une meilleure rentabilité de leur épargne en la mettant au service de l'économie réelle, le tout simplement grâce à ces plateformes dont la petite commission est bien inférieure à la marge d'intérêt et aux frais dont se gavent les banques.

Plus besoin de banques ! L'idée est séduisante et bénéficie d'un capital de sympathie indiscutable vis-à-vis du public enthousiaste. Qu'on en juge : 1,5 million de Français auraient prêté 85,2 millions d'euros, investi 24,3 millions d'euros ou soutenu un projet avec 23,7 millions d'euros de dons (dont 20 millions « avec récompense » c'est-à-dire contre un produit ou service), dans le cadre d'opérations de crowdfunding au premier semestre 2015, soit deux fois plus qu'au premier semestre 2014, selon le dernier baromètre de l'association Financement Participatif France.

Il faut dire que le financement participatif, qui était longtemps hors-la-loi au regard des réglementations financières, a bénéficié d'une réglementation allégée légalisant et facilitant son développement, comme Deontofi.com l'avait évoqué dès 2014.

« En France, l'ordonnance du 30 Mai 2014 et le décret du 16 septembre 2014 relatifs au financement participatif ont régulé le secteur du prêt et de l'investissement participatifs en instaurant deux statuts spécifiques (intermédiaire en financement participatif pour le prêt et conseiller en investissements participatifs pour l'investissement) qui permettent aux plateformes respectant la législation de bénéficier d'un label. Le gouvernement a ainsi à plusieurs reprises affiché sa volonté de faire de la France le pays leader du crowdfunding, qui rencontre en effet particulièrement de succès dans l'Hexagone », explique ainsi le ministère de l'écologie, du développement durable et de l'énergie sur son site Internet.

Difficile dans ces conditions de mettre en garde les épargnants contre les risques d'arnaques au crowdfunding, sans passer pour un ringard réac défendant le pré-carré des banques. Les lecteurs de Deontofi.com savent bien que ce site d'information n'est pas complaisant avec les lobbies bancaires.

Le problème est que le crowdfunding, sous son visage sympathique, est aussi un boulevard facilitant l'accès de nombreux escrocs à l'épargne publique. Il suffit de s'inventer un projet écolo, ou techno, ou d'entrepreneuriat social dans la tendance du moment, ou au contraire miser sur l'appât du gain avec un mirage immobilier ou n'importe quel château en Espagne,

pour convaincre les épargnants confiants de donner leurs économies en échange d'une promesse de rendement élevé pour couronner le tout.

La recette est d'une banalité aussi affligeante qu'efficace, car c'est bien la même qui a permis à la plateforme de financement participatif chinoise Ezubao de collecter 7 milliards d'euros auprès de 900 000 épargnants, en leur promettant des taux d'intérêt entre 9% et 14,5% sur des prêts à d'improbables entreprises fictives.

Près d'un million d'épargnants ne reverront jamais leur argent

L'arrestation du fondateur d'Ezubao, le jeune Ding Ning (34 ans) et d'une vingtaine de ses employés, à Pékin dimanche 29 janvier 2016, a révélé au monde que tout était faux. La start-up était devenue leader chinois du financement participatif en dix-huit mois, à grand renfort de publicités, en engloutissant l'épargne de ses derniers pigeons pour entretenir l'illusion de rentabilité promise aux pigeons précédents dont le capital ne serait jamais remboursable. Quand cette spirale n'a plus trouvé assez de pigeons pour s'entretenir, elle s'est écroulée.

C'est ce qu'on appelle un système d'épargne pyramidal, ou encore système de Ponzi, redevenu célèbre au XXIème Siècle grâce aux prouesses de Bernard Madoff, incontestable recordman de l'escroquerie pyramidale.

Encore une fois, Deontofi.com n'est évidemment pas opposé aux vertus du crowdfunding. D'ailleurs, qui peut l'être ? Mais notre devoir est de mettre en garde les épargnants sur les risques de déceptions liées aux espoirs qu'ils fondent sur le financement participatif, car beaucoup ne reverront jamais leur argent ni même les intérêts ou formidables gains promis.

<https://deontofi.com/coup-dur-pour-la-finance-participative-900-000-epargnants-floues/>

Pégase, le cheval ailé qui vole (les épargnants) et s'évapore avec leur argent !

Alors que le gendarme boursier alerte les épargnants sur le retrait d'agrément d'un escroc régulé du trading Forex, les sites de ce courtier chypriote, le bien nommé Pegase Capital Ltd, se sont évaporés avec l'argent des clients.

Le gendarme boursier alerte les épargnants qu'une poignée de sites de trading appartenant au courtier chypriote Pegase Capital Ltd mettent la clé sous la porte. Prise en flagrant délit de tromperie, ce voleur chypriote séduisait les épargnants français en revendiquant son caractère régulé, avec un agrément. Mais son comportement n'avait rien d'un courtier régulé. Ses activités n'étaient absolument pas conformes à l'agrément qu'il affichait pour mieux tromper les épargnants. Le gendarme boursier chypriote, la Cysec, avait donc « suspendu » l'agrément de Pegase Capital depuis le 4 mars 2016, dans l'attente des améliorations nécessaires pour mériter réellement cet agrément. Illusoire, bien sûr !

Un escroc ayant pris un déguisement d'intermédiaire régulé n'a ni l'envie ni la capacité à se mettre en conformité avec les règles, car elles sont incompatibles avec son modèle d'enrichissement basé sur le détournement d'argent.

Sentant le vent tourner, Pegase Capital a préféré abandonner définitivement son statut d'escroc régulé, en renonçant à son fameux agrément chypriote...

Résultat, le cheval ailé s'est envolé, car Pegase sait très bien voler. Il suffit de lire la mythologie grecque pour comprendre qu'il a volé et trompé les mortels épargnants impressionnés par son agrément de voleur régulé, pour rejoindre Zeus qui l'a transformé en constellation d'étoile.

En clair, les épargnants qui sont invités à retirer leur argent n'ont probablement guère de chance de revoir la moindre poussière de centime de leurs économies. Les sites internet de

trading litigieux ont déjà disparu du cyber-espace, et l'AMF n'est même pas sûr que l'écurie dudit cheval volant soit encore à la même adresse.

L'argent placé chez cet escroc régulé s'est probablement aussi évaporé dans les étoiles, sur les ailes de Pégase qui l'a volé.

Le conseil de Deontofi.com : **NE PLACEZ JAMAIS D'ARGENT CHEZ UN COURTIER CHYPRIOTE** !

Les sites de trading « régulés » sont des escroqueries régulées. Vous avez la garantie de perdre votre argent.

ATTENTION : cette opinion est valable aussi pour les sites de trading sponsors des clubs de foot !!! Vous ne reverrez jamais l'argent que vous leur confiez.

<https://deontofi.com/pegase-le-cheval-aile-qui-vole-les-epargnants-et-sevapore-dans-les-etoiles/>

Même les geeks se méfient de l'e-monnaie

Jusqu'à l'éclatement de l'affaire Liberty Reserve, cette société américaine de transferts de fonds sur Internet, aujourd'hui soupçonnée de blanchiment d'argent à hauteur de 6 milliards de dollars (4,6 milliards d'euros), peu de gens connaissaient l'existence des monnaies électroniques, ni leur mode de fonctionnement.

En quelques jours, on a découvert la dimension de ces nouveaux instruments monétaires. Dans la foulée ont émergé les noms des champions de ces monnaies virtuelles : Mt. Gox, la "Bourse d'échange" numéro un du circuit, et d'autres aux noms aussi "numériques" (Bitomat, Bitfloor...) que leur monnaie : Bitcoin, Litecoin, SolidCoin, GeistGeld, Ripple, BBQCoin... Ces sociétés ne sont pas qu'américaines : on en trouve à Moscou (WebMoney), au Panama (Perfect Money)... Au Proche-Orient, la plus connue s'appelle cashU. En 2011, quand elle a senti le souffle de la justice dans son dos, Liberty Reserve s'était délocalisée au Costa Rica. Pour l'anecdote, la première tentative d'acheter des biens sur Internet en "monnaie virtuelle" remonte à 1999, lorsqu'une devise du nom de Flooz fit brièvement son apparition. La prononciation à l'anglaise ("flouze") avait un petit côté provocant et sans équivoque.

Mais si chaque plate-forme de transfert d'argent dispose aujourd'hui de sa propre "monnaie virtuelle", la plus célèbre se nomme Bitcoin, première du genre à s'être imposée. C'était il y a quatre ans seulement. Il n'est vraisemblablement pas anodin que le nom de son ou de ses inventeurs soit lui-même resté jusqu'à ce jour inconnu ! Satoshi Nakamoto, auteur du premier post sur le Web expliquant le fonctionnement de Bitcoin, le 24 mai 2009, s'est révélé n'être qu'un pseudonyme.

Le *New Yorker* a cherché à découvrir son identité, sans succès. Autant prévenir le lecteur peu averti de la mathématique financière, la lecture du texte (*Bitcoin : A Peer-to-Peer Electronic Cash System*, <http://bitcoin.org/bitcoin.pdf>) est légèrement absconse. Bitcoin a ensuite donné naissance à de multiples autres monnaies qui, toutes, fonctionnent sur un principe identique.

JETONS DE CASINO

Ce ne sont pas de "fausses monnaies" : leur détention n'est pas prohibée, on peut les acheter et les vendre, etc. Leur valeur peut même fluctuer en fonction de l'offre et de la demande de leurs "consommateurs".

Ainsi, le Bitcoin s'échangeait entre 2 et 11 euros en 2011-2012, puis a connu une flambée inouïe, grimpant à 110 euros entre février et début avril 2013, puis à 200 euros en une semaine, avant de s'effondrer à 66 euros. Il a ensuite repris son cours haussier et valait 91 euros lundi 3 juin.

Pour sûr, on sent dans ces variations un fumet spéculatif prononcé. Surtout, ces monnaies n'ont de valeur qu'en circuit fermé, un peu comme des jetons de casino. Elles sont "virtuelles",

car sans autre valeur d'usage, comme les jetons, que d'être échangeables contre des devises réelles.

Sont-elles obligatoirement source de trafic ? Pas sûr. Aux Etats-Unis, les sociétés de transfert, pour éviter d'être instrumentalisées "à l'insu de leur plein gré" par des criminels, se disent favorables à une réglementation si elle n'empiète pas sur leur fonctionnement. Ainsi, contrairement au "LR", la monnaie de Liberty Reserve, la traçabilité de chaque Bitcoin est supposée acquise.

Son principal promoteur, la société Mt. Gox, assure exiger une preuve tangible d'identité et de résidence du client avant d'autoriser une transaction et tenir un registre public de tous ses transferts de fonds. Le problème est que ce n'est pas le cas des autres, et que Mt.Gox est lui-même soupçonné... d'avoir développé des filiales pour se soustraire à sa propre règle.

C'est vraisemblablement parce qu'elles avaient suspecté la propension des promoteurs de ces monnaies et de beaucoup de leurs utilisateurs à y avoir recours pour dissimuler des transactions douteuses que des organisations plutôt favorables au numérique ont progressivement tourné le dos aux monnaies virtuelles.

Ainsi de WikiLeaks, qui n'accepte plus les dons en monnaie virtuelle. Ou de Facebook. En 2009, le réseau social a offert à ses membres d'utiliser des "Facebook Credits", mais coupa rapidement court à cette pratique.

http://www.lemonde.fr/economie/article/2013/06/04/meme-les-geeks-se-mefient-de-l-e-monnaie_3423395_3234.html