Internet au service de la criminalité économique?

Autor(en): **Ricca, Marco**

Objekttyp: **Article**

Zeitschrift: **Revue économique et sociale : bulletin de la Société d'Etudes Economiques et Sociales**

Band (Jahr): **61 (2003)**

Heft 3: **Lutte contre la criminalité économique : prévenir, détecter, réprimer**

PDF erstellt am: **21.09.2024**

Persistenter Link: https://doi.org/10.5169/seals-141369

INTERNET AU SERVICE DE LA CRIMINALITÉ ÉCONOMIQUE ?

Marco RICCA
Cofondateur ILION Security SA
http://www.ilionsecurity.ch
marco.ricca@hpl.hp.com

La société moderne a vu évoluer ces dernières années des technologies qui peuvent susciter un certain nombre d'interrogations quant à leur utilisation pour perpétrer des délits relevant de la criminalité économique.

En illustrant certains des mécanismes qui, en s'appuyant sur ces nouvelles technologies, facilitent ou même parfois rendent possible ce type de criminalité, on tentera d'évaluer dans quelle mesure on peut leur imputer la faute de servir la délinquance financière.

Le terme de *criminalité économique* peut s'appliquer à une vaste palette de délits ; en effet, on peut ainsi désigner aussi bien les petites arnaques à la carte de crédit, portant sur quelques dizaines de milliers de francs, que le blanchiment de capitaux, dont les sommes en jeu dépassent souvent des quantités à six zéros. On peut s'attendre par conséquent à ce que les technologies employées varient fortement en fonction du délit considéré.

Le réseau Internet fait partie de ces nouvelles technologies qui ont considérablement augmenté le confort moyen de l'individu ; les derniers chiffres indiquent qu'au total dans le monde un peu plus de 600 millions de personnes ont fait usage d'Internet au cours des trois derniers mois *(source : NUA Internet Surveys, Septembre 2002)* et ont donc ainsi pu bénéficier d'un ensemble de prestations leur permettant d'économiser du temps pour obtenir une information, un produit ou un service. Le revers de la médaille consiste évidemment dans le fait que les arnaques pullulent sur Internet ; beaucoup de personnes peu scrupuleuses se servent de ce média pour flouer le consommateur et lui soustraire illégalement des fonds.

Le problème a atteint une telle ampleur que la police fédérale américaine a dû mettre sur pied un service dédié à l'unique tâche de répertorier et, dans la mesure du possible, traquer ce genre d'activités délictueuses *(IFCC – Internet Fraud Complaint Center – www.ifccfbi.gov)*. Cette organisation recense des délits aussi variés que la fraude à l'investissement – des sites Web proposent des placements à des taux alléchants, avant de disparaître avec les capitaux –, ou encore l'arnaque à la vente aux enchères – des pseudo vendeurs proposent des articles pour lesquels ils encaissent le payement mais n'expédient jamais le produit –, etc. Le total du préjudice enregistré par cet organisme s'élève à 54 millions de dollars pour l'année 2002, quantité qui ne tient évidemment pas compte des

cas qui ne leur ont pas été dénoncés.

Ce chiffre impressionnant s'explique par le fait qu'Internet présente un certain nombre de caractéristiques qui peuvent incontestablement servir d'atouts aux malfaiteurs ; la première d'entre elles est l'anonymat quasi-garanti du réseau. Il est en effet trivial de parcourir le Web avec la certitude que personne ne peut identifier l'instigateur de la connexion sans investir énormément de temps et d'argent. Il suffit par exemple de se brancher sur un réseau Wireless 802.11b dont les villes modernes regorgent, ou encore plus simplement d'utiliser les services d'un cybercafé. Il existe même des sites souvent gratuits fournissant des services d'anonymisation – *www.anonymizer.com, www.anonymize.net, ou www.triumphpc.com/proxy-server/* pour n'en citer que trois. Cet anonymat concerne également les personnes souhaitant fournir un service via un site Web ; beaucoup de sociétés établies dans des pays à la législation peu regardante proposent d'héberger n'importe quel site sans poser de question, et s'engagent même à détruire les traces qui permettraient d'identifier leurs clients. En plus de garantir aux individus honnêtes la confidentialité à laquelle ils ont droit, cela permet à d'autres d'élaborer des arnaques sans être inquiétés par une quelconque répression.

Ce dernier point illustre une autre caractéristique d'Internet ; le réseau présente le formidable avantage de permettre à des sociétés ou des personnes physiques de communiquer instantanément, où qu'elles se trouvent dans le monde. Malheureusement, cela permet également à des malfaiteurs de dissimuler leurs délits derrière la contrainte souvent fastidieuse de la collaboration entre les législations.

Cette question amène tout naturellement à un autre type de réflexion : dans quelle mesure est-ce qu'Internet facilite le délit économique par excellence : le blanchiment de capitaux ?

Le groupe d'action financière sur le blanchiment de capitaux *(Financial Action Task Force on Money Laundering, www.fatf-gafi.org)*, mis sur pied par l'OCDE pour lutter contre ce fléau, identifie à ce délit toutes les manipulations permettant de dissimuler les origines délictueuses d'un capital, de manière à en profiter sans avoir à en révéler l'origine. Ce même organisme estime la masse d'argent blanchie chaque année dans le monde entre 590 milliards (5.9e11) et 1.5 billions (1.5e12) de dollars.

Avant d'identifier dans quelle mesure le réseau Internet peut servir à un tel crime, il semble pertinent de rappeler comment se déroule une opération classique de blanchiment. En reprenant le vocabulaire anglais couramment employé, on distingue trois phases, à savoir :

- La phase dite de *Placement* : consiste à introduire dans le système financier le capital en espèces obtenu illégalement – comme par exemple créditer un ou plusieurs comptes en banque.
- La phase dite de *Layering* : consiste à déplacer l'argent (le terme ventiler est souvent employé) de manière à lui faire changer de forme et de législation pour brouiller les pistes et obscurcir d'éventuelles tentatives de traçage.

- La phase dite de *Integration* : consiste à rendre leur légitimité aux fonds en les intégrant à un processus financier légal.

La première phase dépend en général de techniques relativement traditionnelles ; le *smurfing* par exemple consiste à diviser le capital et à créditer un grand nombre de comptes en banque un grand nombre de fois, en restant à chaque fois en deçà de la limite à partir de laquelle un contrôle est effectué. Un malfaiteur peut également acheter en espèces des produits de valeur (diamants, or, timbres, art, etc.), et les envoyer à un complice, situé dans une législation moins contraignante, qui se chargera de les revendre et de créditer un compte. On peut encore citer beaucoup d'autres alternatives, comme les virements bancaires anonymes proposés par beaucoup de bureaux de poste ; toutefois peu d'entre elles se servent réellement d'Internet ; cette phase du délit nécessite en général une interaction pour introduire de l'argent liquide dans le système financier.

Les deux autres étapes sont en revanche beaucoup plus accessibles au commun des mortels depuis l'avènement d'Internet. En effet, alors qu'il fallait autrefois faire appel à des spécialistes plus compétents que scrupuleux, il est désormais possible, par exemple pour faciliter l'étape dite de *Layering*, de solliciter, directement via Internet, les services de sociétés proposant des prestations telles que l'ouverture de sociétés anonymes dans des paradis fiscaux avec gestion de comptes en banque instantanée depuis Internet, cartes de débit internationales fonctionnant sur des comptes complètement anonymes, ou encore adresses fictives depuis lesquelles le courrier est redirigé à son destinataire (parmi ces sociétés de service on cite fréquemment *www.offshore-manual.com*); sans compter les sites de monnaie électronique (*www.e-gold.com, www.e-bullion.com*, etc.) qui sont autant d'outils qui peuvent servir à brouiller les traces de l'argent.

La troisième étape dite de Integration peut également être facilitée notamment par l'intermédiaire des casinos en-ligne ou des sites destinés à jouer en bourse. Une astuce souvent citée consiste par exemple à diviser une somme donnée en deux et à effectuer dans un contexte crédible deux paris distincts et contradictoires ; la somme « perdue » dans le premier pari semblera avoir été légitimement gagnée dans le second.

Comme démontré ci-dessus, Internet facilite dans une certaine mesure certains aspects du blanchiment de capitaux. Il serait toutefois naïf de croire qu'en supprimant ces possibilités on affaiblirait de manière significative ce fléau.

En effet, le phénomène est vieux comme le monde ; l'historien Sterling Seagrave raconte comment, il y a plus de 3000 ans, certains commerçants chinois disposaient de leurs biens de manière à éviter les mesures confiscatoires des autorités de l'époque ; les techniques décrites dans son ouvrage *Lords of the Rims* rappellent clairement celles utilisées à l'heure actuelle – transformation des biens en valeurs facilement transportables et dissimulables, mouvements et investissements dans d'autres législations, ou encore échanges à des prix superficiellement gonflés pour exporter ou importer des fonds.

De surcroît, on peut comparer les nouvelles possibilités offertes par le réseau Internet à l'avènement des *wire transfers*, qui ont certes permis d'accélérer et de mieux dissimuler les transactions,

mais qui ne sont certainement pas à l'origine du problème. Internet n'est rien d'autre qu'un outil qui facilite la communication entre individus et entreprises. Tout devient plus rapide et plus efficace, dont entre autres malheureusement certains aspects du blanchiment de capitaux. Le *cyberlaundering* comme il est appelé n'est pas un problème en soi, puisque ce sont toujours les mêmes principes et raisonnements qui sont appliqués.

Il est toutefois un aspect de la criminalité économique qui est très fortement lié à l'avènement des nouvelles technologies : le piratage informatique. Une institution financière peut en effet craindre qu'un pirate s'introduise dans ses systèmes ; puisque toute l'information est désormais numérisée, il devient trivial, une fois introduit dans un réseau depuis lequel des transactions financières ont lieu, de virer des fonds sur un compte, d'où ils sont par suite ventilés – la seule difficulté consisterait à le faire de manière suffisamment discrète pour maximiser le gain en minimisant la probabilité d'éveiller des soupçons. Puisqu'un tel forfait permet de dérober de l'argent qui se trouve déjà dans le système financier, le malfaiteur évite de surcroît la première étape de blanchiment. Pour se prémunir de tels risques, beaucoup d'institutions financières font désormais appel à des sociétés d'audit telles que *ILION Security SA*, qui emploie des spécialistes capables de simuler une attaque de piratage d'envergure, et ainsi de déceler les faiblesses d'un réseau.

Pour reprendre la question posée au début du texte, le fléau de la criminalité économique ne peut en rien être imputé à l'avènement de nouvelles technologies telles que le réseau Internet. Certes il peut rendre l'accès à l'information plus rapide, ou même faciliter dans une certaine mesure certaines activités délictueuses. Mais de la même manière que des terroristes se servent du téléphone pour mieux planifier leurs attaques, ou des sites Web anarchistes pour fabriquer des bombes plus efficaces, il n'est pas à l'origine du problème.

Notre société moderne a globalisé l'économie, la finance et le commerce, mais pas la loi ; il est extrêmement simple d'entrer en interaction avec une entreprise à l'autre bout de la planète, alors que de solliciter la bureaucratie judiciaire d'un pays même voisin peut s'avérer extrêmement fastidieux. Pour constater l'étendue du paradoxe, il suffit de comparer le temps qu'il faut pour virer des fonds d'un pays à l'autre avec celui nécessaire pour obtenir d'un juge étranger de geler des avoirs.

SOURCES ET RÉFÉRENCES

The Financial Action Task Force on Money Laundering (FATF), http://www.fatf-gafi.org

The Money Laundering Alert Newsletter, http://www.moneylaundering.com/publications.htm

Think Again: Money Laundering, de Nigel Morris-Cotterill, Foreign Policy, Mai/Juin 2001, http://www.foreignpolicy.com

Cyberlaundering : Anonymous Digital Cash and Money Laundering, de R. Mark Bortner, 1996, Université de Miami – Faculté de droit, http://www.law.miami.edu

Crimes of Persuasion : Schemes, scams, frauds, de Les Henderson, Coyote Ridge Publishing, Novembre 2000

Lords of the Rim: The Invisible Empire of the Overseas Chinese, de Sterling Seagrave, Putnam Pub Group

NUA Internet Surveys, http://www.nua.com

Internet Fraud Complaint Center, http://www.ifccfbi.gov