Université Robert Schuman

Strasbourg - Faculté de droit

La contribution de l'Union européenne à la lutte contre le trafic de données personnelles sur Internet

Mémoire sous la direction de Mme Juliette Lelieur

- Lutte contre la criminalité organisée -

Amélie Deleuze

Master 2 Droit pénal de l'Union européenne

Soutenance, le 10 septembre 2015

Jury : Olivier Cahn, maître de conférences à l'Université de Cergy-Pontoise

et Juliette Lelieur, maître de conférences à l'Université de Strasbourg

Année 2014/2015

Je montrerai à ces gens ce que vous ne voulez pas qu'ils voient. Je leur ferai voir un monde sans vous, un monde sans lois ni contrôle, sans limites ni frontières, un monde où tout est possible. Ce que nous en ferons ne dépendra que de vous.

- « Matrix », des frères Wachowski, 1999 (Australie, États-Unis) -

Au moment de rendre ce mémoire, je voudrais remercier ma famille, mon père pour ses corrections détaillées, mes deux incroyables petites sœurs, Camille et Lucie, et surtout ma mère, dont j'aimerais qu'elle soit encore là. Merci également à Me Juliette Lelieur, pour sa supervision de chaque instant, et ce malgré son immobilisation temporaire. Mes remerciements les plus sincères à tout le personnel du tribunal de grande instance de Nanterre, dont surtout ma maître de stage, Inès da Camara, mes meilleurs vœux l'accompagnent.

Sommaire

Abréviations

AGRASC - Agence de Gestion et de Recouvrement des Avoirs Saisis et Confisqués

ARO - Bureaux de recouvrement des avoirs (Assets Recovery Office)

BCE - Banque Centrale Européenne

C2C - Du Crime au Crime

CANAFE - Centre d'analyse des opérations et déclarations financières du Canada

CARIN - Camden Asset Recovery Inter-agency Network

Cass. Civ. - Chambre civile de la Cour de cassation

Cass. Crim. - Chambre criminelle de la Cour de cassation

CEDH - Cour Européenne des Droits de l'Homme

CEIS - Compagnie Européenne d'Intelligence Stratégique

CEPC - Comité européen pour les problèmes criminels

CEPOL - Collège Européen de POLice

CJUE - Cour de Justice de l'Union européenne

CNIL - Commission Nationale Informatique et Libertés

CNSA - Accord de coopération du réseau de contact des autorités anti-spam

COSI - Comité permanent de coopération Opérationnelle en matière de Sécurité Intérieure

CREOGN - Centre de Recherche de l'École des Officiers de la Gendarmerie Nationale

DDoS - Distributed Denial of Service

DUDH - Déclaration universelle des droits de l'Homme

EC3 - Centre Européen de Cybercriminalité (European Cybercrime Centre)

ECTEG - European Cybercrime Training and Education Group

EGBA - European Gaming and Betting Association

EUCTF - European Union Cybercrime Taskforce

Eurojust - Unité de coopération judiciaire de l'Union européenne

Europol - Office EURopéen de POLice

FAI - Fournisseurs d'Accès à Internet

FBI - Federal Bureau of Investigation

FinCEN - Financial Crimes Enforcement Network

FSI - Fournisseurs de Services Internet

GAFI - Groupe d'Action Financière

ICANN - Internet Corporation for Assigned Names and Numbers

IDC - International Data Corporation

Interpol - OIPC Organisation internationale de police criminelle

iOCTA - Internet Organised Crime Threat Assessment

IP - Internet Protocole

IRL - In Real Life

ISS - Institut d'Études de Sécurité

ITU - Union Internationale des Télécommunications (International Telecommunications Unions)

IWF - Internet Watch Foundation

LICRA - Ligue Contre le Racisme et l'Antisémitisme

MAE - Mandat d'arrêt européen

MMORPG - Jeux de rôle en ligne rassemblant beaucoup de joueurs (Massively Multiplayer Online Role Playing Games)

NMP - Nouvelles Méthodes de Paiement

OCDE Organisation de Coopération et de Développement Économiques

OCRGDF - Office Central pour la Répression de la Grande Délinquance Financière

ONUDC - Office des Nations Unies contre la Drogue et le Crime

OSCE - Organisation pour la sécurité et la coopération en Europe

PIAC - Plateforme d'Identification des Avoirs Criminels

RAT - Remote Access Trojan

SEA - Armée Electronique Syrienne (Syrian Electronic Army)

SEAE - Service européen pour l'action extérieure

SEO - Search engine optimization

STAR - Stolen Asset Recovery

TFUE - Traité sur le Fonctionnement de l'Union européenne

TRACFIN - Cellule de Traitement du Renseignement et Action contre les Circuits FINanciers clandestins

TOR - The Onion Router

UE - Union européenne

UEJF - Union des Étudiants Juifs de France

VBV - Identifiants bancaires (Verified By Visa)

WOW - World of Warcraft

Introduction

Les pirates informatiques et les *hacktivistes* nous annoncent un monde où l'information est libre, gratuite.[1] Les médias, dont l'activité est axée sur la création et la transmission de données propriétaires, nous avertissent des dangers d'un tel univers.[2] La capacité à s'approprier les données que l'on produit est un des moteurs de leur création, la dénonciation d'une telle propriété reviendrait donc à miner les activités de création et de traitement des données.

Ce débat autour de la libéralisation de l'accès aux informations touche à notre quotidien dès-lors que l'on parle de données personnelles, ces informations qui constituent notre identité.[3]

Cette notion d'identité n'a longtemps eu de réalité que dans les relations interpersonnelles de l'individu. Elle est entrée en droit avec la notion de personnalité, modèle agrégateur de notre patrimoine et de nos droits. Au cours du 19ème siècle, les États l'ont aussi exploitée par l'identification, la mettant au service de la sécurité et de l'ordre social. L'Europe est entrée dans l'ère des papiers d'identité, du fichage, du traçage, etc. Le bertillonnage et l'étude des empreintes digitales se sont développés, et avec eux l'idée qu'un certain nombre de caractères, qu'un certain nombre d'informations pouvaient garantir l'identification.

Avec l'émergence d'Internet, il a fallu concevoir de nouvelles méthodes. Nous avons sélectionné un certain nombre de données, à la fois individuelles et dématérialisables : ce sont nos numéros de sécurité sociale, nos adresses mails ou encore nos identifiants bancaires. Ces données personnelles particulières sont à la fois une part de notre identité et la clé qui permet d'y accéder. L'identification s'en est trouvée fluidifiée mais l'identité en est ressortie vulnérable.[4]

Il est en effet très difficile de protéger une information. Elles se volent par réplication, procédé qui n'alerte pas toujours les victimes. Or, à mesure que des activités en nombre croissant se dématérialisent, le vol, le trafic et l'utilisation frauduleuse des données personnelles ne peuvent qu'attirer davantage de criminels. Par le biais de ces données, c'est l'identité toute entière de l'individu qui est susceptible d'une exploitation.[5]

Face à ce bouleversement, on ne peut que constater la relative réactivité des législateurs des

1 Conformément à la devise du groupe d'*hacktivistes Anonymous* : « *Knowledge is free. We are Anonymous. We are Legion. We do not forgive. We do not forget. Expect us.* » (« *La connaissance est gratuite. Nous sommes Anonymous. Nous sommes légion. Nous ne pardonnons pas. Nous n'oublions pas. Redoutez-nous.* »).
2 Voir lexique, entrées **Données**, **Donnée personnelle**, **Données propriétaires** et **Données publiques**.
3 Voir lexique, entrée **Identité**.
4 PIERRE Julien, *Génétique de l'identité numérique. Sources et enjeux des processus associés à l'identité numérique*, Les Cahiers du numérique 1/2011 (Vol. 7) , p. 15-29 (consulté le 20 novembre 2015) www.cairn.info/revue-les-cahiers-du-numerique-2011-1-page-15.htm.
5 Informations bancaires, historiques professionnels, papiers d'identité, etc.

États membres de l'Union européenne (UE).

La seule révolution comparable de notre conception de l'information est l'invention de l'imprimerie, au milieu du quinzième siècle. Elle avait entraîné la diffusion en masse du livre et l'apparition du journalisme écrit. Il avait alors fallu attendre le dix-huitième siècle pour voir ces mêmes législateurs aménager un droit d'auteur en réponse.[67]

L'existence d'une réaction de l'ensemble des législateurs européens, moins d'une génération après l'ouverture au public d'Internet, a interpellé la doctrine, qui a cru à un changement du mode de gouvernement ou à une nature particulière de la révolution numérique.[8]

L'explication semble bien plutôt être d'ordre économique. Internet a changé l'ensemble de nos comportements. Avant d'introduire de nouvelles formes de criminalité, il a surtout créé un nouveau secteur d'économie, où l'information est le premier produit d'échange. Quand une majeure partie de notre société a basculé en ligne, nos législateurs ont naturellement proposé un cadre qui protège notre vie informatique.

Peut-être n'est-il pas étonnant que, dans la hâte, ils n'aient pas encore délimité précisément la cybercriminalité. Ils y ont souvent inclus pêle-mêle les infractions strictement informatiques qui ont pour cibles les systèmes d'information, les systèmes de traitement informatisé des données, ainsi que des infractions classiques (souvent la fraude ou l'escroquerie) facilitées ou démultipliées par le recours à Internet.[9]

Dans ce champ extrêmement large, le législateur a néanmoins pris la peine de protéger tout particulièrement ce qu'il qualifie de « données à caractère personnel ». L'UE a été visionnaire en la matière : elle a adoptée une directive en la matière dès 1995 et elle a inséré la protection des données personnelles parmi les droits fondamentaux dont elle s'impose le respect.[10]

Cette protection, initialement conçue comme un encadrement des acteurs privés, tend à s'imposer

6 En France, les premiers textes de loi sont adoptés en 1791 et 1793.
7 GYORY Michel, *Le droit d'auteur face aux révolutions technologiques*, Revue en ligne Bon-A-Tirer, 2010 [en ligne] (consulté le 20 août 2015) http://www.bon-a-tirer.com/volume145/gyory.html.
8 Philippe Charepie et Alain Le Diberder, pour la France, offrent par exemple une analyse très synthétique de cette révolution (CHANTEPIE Philippe, LE DIBERDER Alain, « I. Le nouveau paysage numérique » et « IV. L'exploitation numérique : tout change », *Révolution numérique et industries culturelles*, Paris, La Découverte , «Repères», 2010, 128 p.). D'autres auteurs ont mis en lumière la profonde mutation du droit d'auteur dans le contexte de cette nouvelle société, dite « de l'information » (Dusollier Séverine, *Les mesures techniques dans la directive sur le droit d'auteur dans la société de l'information : un délicat compromis*, LEGICOM 2/2001 (N° 25) , p. 75-86).
Cette doctrine de la révolution numérique peut d'ailleurs offrir une perspective moins pessimiste que celle de l'industrie culturelle sur la libéralisation de l'information. Ainsi, par exemple, d'aucuns n'a pas hésité à dire que ce qui était dénoncé comme une dévalorisation de l'activité de production d'information n'était que sa libéralisation (MAUREL Lionel, *Droit d'auteur et création dans l'environnement numérique. Des conditions d'émancipation à repenser d'urgence*, Mouvements 3/2014 (n° 79) , p. 100-108, par exemple).
9 Voir lexique, entrée **STAD**.
10 Union européenne, *Charte des droits fondamentaux*, article 8.

aux autorités publiques depuis juin 2013 et le début de l'affaire Snowden. L'Union européenne élabore d'ailleurs un règlement qui devrait compléter son dispositif sur ce point.[11]

Cette législation européenne a directement inspiré les lois élaborées dans d'autres pays et sur d'autres continents. Le Québec, par exemple, a adopté une législation sur les données personnelles directement inspirée du droit de l'UE.[12]

L'Union n'a pas encore traité du volet pénal de la protection de notre identité. Elle n'envisage le trafic de données personnelles qu'au titre de son appartenance à la cybercriminalité. Il s'agit pourtant d'une branche singulière de ce phénomène criminel : les trafiquants de données personnelles en lignes sont des cybercriminels particuliers, motivés exclusivement par des fins mercenaires.

Peut-être est-ce là son talon d'Achille. Depuis une dizaine d'années, les professionnels européens envisage l'investigation financière, incluant l'identification, le gel et la saisie des avoirs criminels, comme un biais remarquable pour lutter contre la criminalité organisée. En effet, il s'agit tant d'une méthode de preuve que d'un moyen dissuasif et à même d'assurer le démantèlement des réseaux visés.

Un coup fatal pourrait être porté aux réseaux d'échange de données personnelles par cette méthode d'investigation, caractérisée par l'analyse d'éléments matériels économiques et financiers à tous les stades des enquêtes dans une démarche forensique de façon à recueillir des preuves des infractions et à identifier leurs auteurs pour identifier et saisir les produits du crime.

L'UE se trouve dans une position idéale pour inspirer une rénovation globale de la protection des données personnelles. Avec 28 États-membres parmi les mieux pénétrants sur Internet et une population largement victime sur ce même réseau, elle est aussi apte à lancer une réponse globale à cette forme de criminalité transnationale et déterritorialisée.

Non seulement elle peut promouvoir les coopérations policières et judiciaires à l'intérieur de ses frontières, mais elle entretient des relations internationales suivies, tant avec d'autres États cibles (États-Unis, par exemple) qu'avec les États d'origine des cybercriminels (Asie-Pacifique, Afrique subsaharienne et monde russophone). Elle se trouve dans une position idéale pour la promotion d'initiatives internationales, ainsi que pour la passation d'accords internationaux en matière d'enquête, de poursuite et d'exécution des décisions de justice.

Comment l'Union européenne peut-elle faciliter la lutte contre le trafic de données personnelles sur

11 LEFEBURE Antoine, *L'affaire Snowden. Comment les États-Unis espionnent le monde*, La Découverte, Paris, février 2014, 275 pp..
12 Canada (Québec), *Loi sur la protection des renseignements personnels dans le secteur privé* (L.R.Q., chapitre P-39.1).

Internet, aux stades de l'investigation, des poursuites mais aussi de l'exécution des décisions, en particulier dans la perspective de priver ces réseaux criminels de leurs moyens financiers ?

Cette étude sera divisée en trois temps. Premièrement, nous verrons quels défis les services d'enquête et de poursuite doivent surmonter pour mettre fin à ce trafic (**Partie I**). Les objets, les moyens et les pratiquants de cette criminalité ne sont pas encore suffisamment définis à l'échelle de l'UE. Ce phénomène pose également des problèmes d'identification des victimes, de recueil de la preuve ou liés à son caractère transfrontalier.

Ensuite, dans la perspective d'une lutte axée sur l'investigation financière, nous étudierons les spécificités économiques du trafic (**Partie II**). Nous verrons qu'il est surtout le fait de réseaux très structurés échangeant les données personnelles, les moyens de se les procurer ou de les utiliser par le biais de marchés noirs formant une économie du service où règne la demande et où la concurrence féroce favorise les opérateurs pouvant proposer la meilleure offre. Alors que l'anonymat de rigueur pourrait donner à ces échanges l'air clandestin, des intermédiaires restent accessibles à l'investigation et aux poursuites, à l'exemple des spammeurs, et les gains réalisés sur Internet doivent encore être réintroduits dans l'économie classique.

Enfin, nous nous pencherons sur les apports de l'Union européenne en termes de coordination des organes d'investigation et de poursuite mais aussi de promotion de l'investigation financière (**Partie III**). Elle a déjà joué un rôle de prime importance dans cette coordination, tant à l'intérieur que hors des frontières de l'UE. Alors que ses différents organes ont pris position pour la systématisation du recours à l'investigation financière dans les cas de trafic de données personnelles, comme dans toute la criminalité organisée, elle devra permettre à l'enquêteur de s'adapter aux moyens de blanchiment d'argent spécifiques au cyberdélinquant.

Partie I : Les difficultés de la lutte contre le trafic de données personnelles sur Internet

L'informatique s'impose comme le moyen principal d'échange d'informations. Elle constitue donc un terrain majeur de vol et d'utilisation frauduleuse des données personnelles. Dans la lutte contre ceux-ci, les cybercriminels constituent une cible pour la police et la justice. Ces dernières se heurtent malheureusement à plusieurs obstacles sévères. Le moindre de ceux-ci n'est pas l'indéfinition du phénomène (**Titre I**). S'y ajoutent de nombreuses difficultés liées à l'enquête, à la preuve et à l'exécution des décisions de justice (**Titre II**).

Titre I : Le trafic de données personnelles sur Internet, un phénomène mal-défini

Comment lutter efficacement contre le trafic de données personnelles par Internet, quand l'objet reste difficile à définir (**Chapitre 1**), quand les infractions informatiques qui en ressortent ne sont pas également définies et punies dans tous les États (**Chapitre 2**) et quand il manque souvent aux législateurs une compréhension de base du monde occulte des *hackers* (**Chapitre 3**) ?

Chapitre 1 : Les données personnelles comme cibles du cybercriminel

La question particulière de pénaliser le vol et les usages frauduleux de données personnelles est compliquée par l'incapacité des législateurs nationaux à s'entendre sur leur définition (*section 1*), handicap qui ne ralentit pas les cybercriminels (*section 2*) dans leur collecte illicite (*section 3*).

Section 1 : Les incertitudes sur la définition des données personnelles

Est une donnée personnelle toute information relative à une personne physique identifiée ou susceptible de l'être, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres.

Cette définition est celle de l'Union européenne, posée dans la directive 95/46/CE du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données. L'utilisation de la directive limite l'harmonisation

des législations nationales en se refusant à fixer les moyens de la protection. La transposition par les États membres de cette définition a varié. Alors que certains, comme la France, l'ont reproduite dans toute sa largeur, d'autres, au premier rang desquels le Royaume-Uni, se sont efforcés de la borner.[13]

Au Royaume-Uni, la transposition des dispositions européennes est passée par l'adoption du *Data Protection Act* de 1998, en vigueur depuis mars 2000 et amendé plusieurs fois, qui met en place l'*Information Commissioner's Office* (ICO), organisme chargé du respect de la protection des données. Le premier article de cette loi britannique énonce la définition suivante :

« *"personal data" means data which relate to a living individual who can be identified (a) from those data, or (b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.* »[14]

Cette loi se concentre donc sur la donnée personnelle constituée par une opinion sur l'individu ou une intention le concernant, lui, ou une personne avec qui il est lié. Les tribunaux britanniques ont limité cette définition aux données touchant à la vie privée de l'individu, notamment via une décision Durant.[15] Malgré les tentatives de conciliation ou de correction de l'autorité de protection des données britannique et de l'UE, cette position a été confirmée en 2008 par les cours britanniques.[16]

En France, la transposition a été réalisée par la réforme de la loi « Informatique et libertés »[17] qui crée la Commission Nationale Informatique et Libertés (CNIL).[18] Son article 2 est mot pour mot conforme à la directive. La CNIL assure un niveau élevé de protection, qui se traduit par le traitement d'un nombre élevé de plaintes, bien réparties par secteurs, comme l'illustrent les

13 PAPACOSTAS Melina, *Projet de réforme européenne sur la protection des données personnelles, enjeux français et anglais*, Université Paris Ouest Nanterre La Défense - Société de l'information, droits et médias, 21 avril 2013 [en ligne] (page consulté le 20 août 2015) http://m2bde.u-paris10.fr/node/2515?destination=node%2F2515.

14 « *On entend par le terme « données personnelles » toute donnée liée à un individu, vivant et pouvant être identifié : a) par cette donnée ou b) par cette donnée, associée à toute information en sa possession ou susceptible de l'être, et inclut toute expression d'une opinion concernant ledit individu et toute indication des intentions du responsable de son traitement ou de toute autre personne quant à cet individu.* »

15 EWCA Civ. (Royaume-Uni), 2003, n°1746, *Michael John Durant v Financial Services Authority*, [en ligne] (consulté le 20 août 2015) https://www.gov.im/lib/docs/odps/cl_durantvsfsa.pdf, paragraphe 28 : « *not all information retrieved from a computer search against an individual's name or unique identifier is personal data within the Act.* [...] *In short, it is information that affects his privacy, whether in his personal or family life, business or professional capacity.* »

16 Court of Session, Inner House, First Division (Écosse), 1er décembre 2006, *Common Services Agency v Scottish Information Commissioner* ([2006] CSIH 58; 2007 S.C. 231; 2007 S.L.T. 7; 2006 G.W.D. 39-766).

17 *Loi n° 78-17 relative à l'informatique, aux fichiers et aux libertés*, 6 janvier 1978 (Journal officiel du 7 janvier 1978 et rectificatif au J.O. du 25 janvier 1978).

18 *Loi n° 2004-801 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel*, 6 août 2004 (JO n° 182 du 7 août 2004).

graphiques des annexes 4 et 5.[19]

Néanmoins, même au sein d'un État, la définition des données personnelles est plus ou moins inclusive suivant qu'on s'adresse à l'autorité chargée de leur protection ou à une juridiction. Ainsi, en France, un cas oppose la CNIL à la Cour de cassation : l'adresse *IP*.[20] Selon un arrêt de 2009, une autorisation préalable de la CNIL n'est pas nécessaire pour recueillir les adresses *IP* des visiteurs d'un site Internet, ce qui tend à affirmer qu'il ne s'agit pas de données personnelles,[21] conclusion à laquelle la CNIL s'oppose fermement,[22] de même que la Commission Européenne.[23]

La notion de donnée personnelle varie, d'un État membre à l'autre mais aussi à l'intérieur de chacun. Or, la qualification de données personnelles entraîne tout un éventail de conséquences, quant aux modalités de leur transfert comme de leur traitement. Une définition élargie accroît le niveau de protection mais complique le transfert et le traitement. Au contraire, une définition étroite facilite le commerce de ces données, à l'heure où leur valeur ne cesse de croître.

Section 2 : Les données personnelles, un produit de valeur

Les spécialistes de la donnée[24] constatent qu'elle connaît un vrai regain de valeur depuis le début des années 2000. Ils attribuent cette popularité à l'entrée dans l'ère du *Big Data* et à l'explosion du volume des données disponibles. Face à cette croissance, les professionnels qui dépendent de l'exactitude de leurs « données consommateurs » doivent se reposer sur des sociétés dont l'activité principale est le filtrage des informations, un procédé ancien, dont les courtiers en données estiment qu'il est apparu dans les années 80.[25] L'enjeu principal est le marketing.

Ces *data brokers* pratiquent ouvertement une activité équivalente à celle des trafiquants de données personnelles, qui peut les amener à violer le principe de transparence de la collecte et du traitement de ces données. Pour des raisons pratiques, nous n'inclurons pas ces professionnels aux activités semi-légales dans notre étude des réseaux cybercriminels de captation, d'échange et d'utilisation des

19 Voir **Annexe 4 : Répartition par secteur des plaintes déposées à la CNIL** et **Annexe 5 : Evolution des demandes de consultation indirecte à la CNIL**.
20 Voir lexique, entrée **IP**.
21 Cass. Crim. (France), 16 juin 2009, n° 08-88.560.
22 CNIL, *Le numéro IP*, 30 novembre 2011 [en ligne] (consulté le 20 août 2015) http://www.cil.cnrs.fr/CIL/spip.php?article1463.
23 Parlement Européen, *Réponse donnée par Mme Reding au nom de la Commission*, Question parlementaire P-000873/2013, 12 mars 2013 [en ligne] (consulté le 20 août 2015) http://www.europarl.europa.eu/sides/getAllAnswers.do?reference=P-2013-000873&language=FR.
24 Voir lexique, entrées **Courtier en données** et **Fouille de données**.
25 Voir lexique, entrée **Big data**.

données personnelles.[26]

Les trafiquants influencent quand même ce secteur de l'économie en accélérant la publication des données personnelles. Ils ont causé certaines des plus massives fuites d'informations des dernières décennies. Ils placent non seulement les particuliers mais aussi les plate-formes informatiques des entreprises face à un feu nourri d'attaques. Le nombre de données personnelles publiées à la suite de fuites à l'échelle entrepreneuriale est en augmentation constante.[27] Ces fuites sont peu médiatisées[28] mais, alors que le nombre de données perdues ou publiées par un employé n'a cessé de diminuer depuis dix ans, le nombre de données *hackées* a explosé.

La quantité de données personnelles a augmenté au point d'alimenter des catalogues. Les trafiquants revendent les données personnelles à l'unité ou sous la forme d'un produit correspondant aux besoins de l'acheteur : informations bancaires, de crédit, faux passeports, fausses cartes d'identité, faux permis de conduire, *fullz*,[29] nouvelles identités prêtes à l'emploi, nouvelles identités et factures justificatives correspondantes[30] ou données d'identité non-raffinées accessibles par un ordinateur, un site ou un réseau infectés. Elles serviront ensuite à mener diverses activités criminelles, dont surtout des fraudes et du blanchiment d'argent.

Chaque item sur ce catalogue est affecté d'un prix moyen, bien connu des spécialistes.[31] Ils constatent sa diminution constante face à un afflux de données. D'où proviennent ces considérables volumes de données personnelles ?

Section 3 : Les moyens d'obtention des données personnelles

Il faut noter que la collecte de données personnelles est plus ancienne que l'informatique.[32] Les nouvelles technologies ont bien apporté une évolution et une modification des modes de collecte mais les techniques mises au point dans les siècles passés sont toujours valables.

26 ROYAKKERS Lambèrs et WEL (van) Lita, *Ethical issues in web data mining*, Ethics and Information Technology, n°6, 2004, pp. 129-140.
27 Voir **Annexe 3 : Infographie des pires fuites de données (2004 -)**.
28 HARBISON Cammy, *10 Largest Data Breaches Of 2014; The Sony Hack Is Not One Of Them*, 26 décembre 2014, iDigital Times [en ligne] (consulté le 20 août 2015) http://www.idigitaltimes.com/10-largest-data-breaches-2014-sony-hack-not-one-them-403219: La fuite de données la plus médiatisée de l'année 2014, celle qui a touché le groupe *Sony*, victime d'attaques attribuées à la Corée du Nord, n'était après tout que la trente-troisième en importance.
29 Voir lexique, entrée **Fullz**.
30 Voir lexique, entrée **Usurpation d'identité**.
31 Voir **Annexe 7 : Valeur des données personnelles *hackées*** et **Annexe 8 : Catalogue des marchés noirs de données personnelles**.
32 VIDOCQ, *Mémoires de Vidocq*, Chef de la police de sûreté jusqu'en 1827, Tome 1, Ebooks libres, 1828, 255 pp. : Déjà au dix-neuvième siècle, Vidocq s'était fait une fortune en recueillant des informations pour les entreprises sur de possibles partenaires financiers. Alors déjà, le détective privé flirtait avec la légalité..

Ainsi, comme l'indique l'infographie des fuites de données placée en annexe 3,[33] une partie non négligeable des fuites est le fait d'utilisateurs des bases de données et d'employés des entreprises. Le recours à l'ingénierie sociale permet toujours la captation de données personnelles. Cette approche est très prisée par les *hackers* qui obtiennent les informations de façon déloyale, en exploitant les failles humaines et sociales d'une structure cible pour atteindre un système informatique. Les spécialistes de l'ingénierie sociale sont similaires aux escrocs classiques car ils utilisent leurs connaissances, leur charisme, des stratagèmes ou leur culot pour parvenir à leurs fins. Ils en diffèrent car ils évitent tout contact physique, ce sont des professionnels du coup de fil ou du mail.[34]

Aujourd'hui, sa traduction la plus commune est le *phishing*, ou hameçonnage, une technique de fraude permettant d'obtenir les données à caractère personnel ou bancaires d'une victime en se faisant passer pour un tiers de confiance.[35]

Un autre moyen de captation de données personnelles est le détournement de connexion vers de faux sites Internet, soit par des biais techniques, pour le *pharming*, soit par le détournement d'une personne ou d'une marque : ce sont le cybersquattage et le *typosquatting*.[36]

Restent l'attaque et l'intrusion informatiques,[37] qui permettent d'accéder à un document, à un site, à un réseau, à un programme ou à une machine, sans l'autorisation nécessaire. Il faut mentionner qu'il existe deux types de cibles. D'une part, il y a les personnes morales, publiques ou privées, qui détiennent un grand nombre de données simultanément. De l'autre, il y a les particuliers. Corrompre leur boîte mail permet d'accéder à une foule d'informations sans prix et corrompre leur ordinateur pour en faire une machine zombie garantit, non seulement l'obtention de nouvelles données, mais aussi la multiplication de la capacité de nuisance du pirate informatique.[38]

L'expédition de *spams* ou encore la perpétration d'attaques par déni de service se trouvent grandement facilitées par l'acquisition de ces *bots*, souvent associés en *botnets*.[39]

Ces moyens de captation ont en commun une certaine furtivité. Le meilleur outil du pirate est celui qui peut être utilisé et réutilisé à l'envi, sans attirer l'attention. Pour cette raison, le trafic d'informations prospère : une donnée est volée par réplication, elle peut exister en deux endroits, la victime ne réalise souvent pas qu'elle a été dépouillée et il a été très compliqué de réprimer ce vol

33 Voir **Annexe 3 : Infographie des pires fuites de données (2004 -)**.
34 Voir lexique, entrée **Ingénierie sociale**.
35 Voir lexique, entrée **Phishing**.
36 Voir lexique, entrées **Pharming** et **Cybersquattage**.
37 Voir lexique, entrée **Attaque informatique** et **Intrusion informatique**.
38 Voir **Annexe 9 : La boîte mail, objet de convoitise dans le monde du *hacking*** et **Annexe 10 : L'ordinateur zombie, un atout de prix dans la manche du *hacker***.
39 Voir lexique, entrée **Zombies**.

d'informations.[40]

40 En France, d'ailleurs, la question de prononcer des condamnations face au phénomène de vol d'informations sur la base de l'article 311-1 du Code pénal (« *Le vol est la soustraction frauduleuse de la chose d'autrui.* ») Pouvait-il en effet y avoir soustraction d'une information ? Avec l'arrêt *Bourquin* (Cour de Cassation, Chambre criminelle, du 12 janvier 1989, 87-82.265, Publié au bulletin), la jurisprudence française semblait parvenue à une solution assez constante : les juges retenaient la qualification de vol s'agissant du support de l'information « volée » et également s'agissant du contenu informationnel de ces supports. Néanmoins, ce vol d'informations n'apparaissait pas susceptible d'être retenu en l'absence d'un support (CA Grenoble, 1e ch. corr., 4 mai 2000, *S. Faibie* c/ *Ministère public et autres*). Un arrêt très récent, rendu le 20 mai 2015, par la chambre criminelle de la Cour de cassation française pourrait bien changer cela (Cass. Crim., 20 mai 2015, 14-81.336, Publié au bulletin). Nous en parlerons plus longuement lorsque nous aborderons l'arsenal législatif français en matière de vol de données personnelles.

Chapitre 2 : La qualification juridique du phénomène de cybercriminalité

Dans le monde, aujourd'hui, un ordinateur sur deux en moyenne serait infecté par un virus.[41] Le nombre de condamnations entrant dans le champ de la cybercriminalité a augmenté régulièrement depuis le début des années 2000 mais reste étonnamment bas, en France au moins.[42] Cette augmentation est loin d'être proportionnelle à celle des fuites de données enregistrées sur la même période.[43] Ce retard serait-il dû à un manque d'appréhension globale du phénomène ? La cybercriminalité est difficile à définir car elle inclut plusieurs types d'infractions (*section 2*), lui étant reliées par divers biais (*section 1*) et susceptibles d'intégrer ou non certains comportements, que la loi, s'ils se déroulaient dans le champ de compétence d'un État, sanctionnerait (*section 3*).

Section 1 : Les différentes branches de la cybercriminalité

Les infractions constituant la cybercriminalité peuvent être divisées en trois grandes catégories : les infractions où le matériel informatique est la cible des auteurs, celles où il est l'outil et celles où il permet de diffuser des contenus numériques illicites ou non souhaités.

Les législateurs de l'UE ont souvent cherché à restreindre la définition de la cybercriminalité. Au Royaume-Uni, par exemple, conformément au *Computer Misuse 1990*, la cybercriminalité s'articule autour de l'accès sans autorisation à un ordinateur ou à des fichiers à données électroniques. Dans d'autres États de l'UE, comme Allemagne, il n'existe pas de définition légale. Les autorités de police de ces deux États ont donc dû réagir et fixer une définition de la cybercriminalité qui recouvre tous les crimes et délits pour la commission desquels Internet a été utilisé.[44]

De même, en France, pour le Ministère de l'Intérieur, la cybercriminalité est l'ensemble des infractions pénales commises via les réseaux informatiques, notamment Internet. Une distinction s'opère entre ces infractions, suivant qu'il s'agit d'atteintes aux biens ou aux personnes.[45]

41 Voir **Annexe 1 : Carte des pays les plus infectés au monde**.
42 Groupe de travail interministériel sur la lutte contre la cybercriminalité, *Protéger les internautes – Rapport sur la cybercriminalité*, février 2014, Annexe 9 – Les statistiques judiciaires, pp. 404-471.
43 Voir **Annexe 3 : Infographie des pires fuites de données (2004 -)**.
44 C'est en tout cas la définition qu'a donnée l'Office fédéral de Police judiciaire allemand. Le *Home Service* a divisé les cybercrimes en plusieurs catégories. La première d'entre elles est celle des infractions spécifiques à la cybercriminalité. Les deux autres sont les infractions utilisant Internet (« *cyber-dependent crime* ») et les infractions démultipliées par Internet (« *cyber-enabled crime* ») : DOWLING Samantha et MCGUIRE Mike, *Cyber crime: A review of the evidence - Summary of key findings and implications*, Home Office Research Report 75, October 2013, 30 pp. (consulté le 20 novembre 2015)
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/246749/horr75-summary.pdf.
45 Ministère de l'Intérieur, *Qu'est-ce-que la cybercriminalité?*, 1er février 2012 [en ligne] (consulté le 20 août 2015)

Les atteintes aux biens incluent, d'une part, les fraudes à la carte bleue sur Internet sans la participation de son titulaire, les ventes par petites annonces ou aux enchères d'objets volés ou contrefaits, les encaissements de paiements sans livraison de la marchandise ou autres escroqueries en tout genre et, d'autre part, le piratage d'ordinateur et la gravure pour soi ou pour autrui de musiques, films ou logiciels. On découvre là une nuance fondamentale, celle entre sanction de comportements perpétrés entièrement en ligne et sanction de comportements physiques.

Les atteintes aux personnes concernent d'abord les contenus, incluant la diffusion d'images pédophiles, de méthodes pour se suicider, de recettes d'explosifs ou d'injures à caractère racial. Elles peuvent ensuite tenir aux récepteurs des contenus, comme les enfants recevant des photographies à caractère pornographique ou violent. Enfin, elles incluent les atteintes à la vie privée.

Une telle typologie couvre les différentes phases du trafic de données personnelles (captation, échange, utilisation abusive) mais apparaît un peu dispersée pour traiter différentes situations de fait qui se sont présentées aux autorités.

Pour une typologie plus rigide, la convention du Conseil de l'Europe sur la cybercriminalité énumère et classe les infractions informatiques fondamentales.[46] Il semble en exister cinq types.

Selon le rapport explicatif de la Convention, le titre 1 sur les infractions contre la confidentialité, l'intégrité et la disponibilité des données et systèmes informatiques vise à contrer les principales menaces pesant sur les STAD. Il va envisager l'accès ou l'interception illégaux, l'atteinte à l'intégrité des données, à l'intégrité du système ou l'abus de dispositifs. Les infractions du titre 2, de fraude et falsification informatiques, ont été inspirées par les travaux du Comité européen pour les problèmes criminels (CEPC). Les infractions du titre 3 se rapportent au contenu. Les rédacteurs du Conseil de l'Europe (CdE) ont envisagé d'y inclure la propagande raciste ou les incitations à la violence mais le comité a résolu de réduire à la seule pornographie enfantine les contenus interdits à la production ou à la diffusion pour des considérations liées à la liberté d'expression. Curieusement, les infractions liées aux atteintes à la propriété intellectuelle et aux droits connexes font l'objet d'un titre 4 distinct.

Le titre 5 de la Convention comprend un article 11 sur la tentative et la complicité et un article 12 sur la responsabilité des personnes morales.

Si le texte vise l'exhaustivité, de l'aveu même des rédacteurs, la Convention laisse aux législateurs nationaux la latitude de prohiber d'autres comportements proche de la cybercriminalité, comme le cybersquattage. Cette diversité a entraîné un éparpillement des dispositions pénales.

http://www.interieur.gouv.fr/A-votre-service/Ma-securite/Conseils-pratiques/Sur-internet/Qu-est-ce-que-la-cybercriminalite.

46 Conseil de l'Europe, *Convention sur la cybercriminalité*, STCE n°185, signée à Budapest, le 23 novembre 2001, entrée en vigueur le 1er juillet 2004.

Section 2 : L'éparpillement des bases légales

La France est à part, même parmi les États membres de l'UE. En effet, la cybercriminalité a été prise juridiquement en compte très précocement, dès la loi relative à l'informatique, aux fichiers et aux libertés du 6 janvier 1978 et de nombreuses dispositions sont venues enrichir l'arsenal législatif à sa disposition pour lutter contre ce phénomène. Pas moins d'une dizaine de textes législatifs a été adoptée dans le domaine.[47] S'y ajoutent une multitude de textes réglementaires et de plans d'action.

Dans d'autres États membres, le législateur s'est efforcé de synthétiser la lutte contre la criminalité informatique en une loi unique, comme le *Computer Misuse Act* britannique.[48] Malgré la définition étroite de la cybercriminalité du Royaume-Uni, cette loi crée quatre infractions d'importance graduée : le simple accès non autorisé à des fichiers informatiques privés à partir d'un autre système, l'accès non autorisé avec l'intention de commettre ou de faciliter la commission d'infractions, les actes non autorisés avec l'intention de nuire ou l'imprudence délibérée dans l'exploitation d'un ordinateur et la création, la fourniture ou l'obtention d'informations afin de les utiliser pour commettre ces infractions. Ces infractions sont donc en général l'accessoire d'autres infractions, d'où un éparpillement de la base juridique d'éventuelles condamnations.

Au moins existe-t-il une définition exhaustive. Aux Pays-Bas, au contraire, le législateur s'est retranché derrière des définitions partielles de la cybercriminalité. Plusieurs catégories de délits existent quand même : atteintes à la confidentialité, à l'intégrité et à la disponibilité des systèmes informatiques, délits traditionnels en lien avec un système informatique, violations de droits d'auteur et de droits assimilés, atteintes à la vie privée ou à la protection des données.

L'Allemagne a choisi également de mettre la donnée au cœur de la cybercriminalité, avec une liste de neuf infractions prévues dans le Code pénal : l'espionnage de données (« *Ausspähen von Daten* », article 202a du Code pénal), la captation de données (« *Abfangen von Daten* », article 202b), la préparation de l'espionnage ou de la captation de données (« *Vorbereiten des Ausspähens*

47 France, *Loi relative à l'informatique, aux fichiers et aux libertés*, 6 janvier 1978 [Loi Informatique et Libertés], *Loi relative à la fraude informatique*, 5 février 1988 [Loi Godfrain], *Loi relative à la sécurité quotidienne*, 15 novembre 2001, *Loi pour la sécurité intérieure*, 18 mars 2003, *Loi portant adaptation de la justice aux évolutions de la criminalité*, 9 mars 2004, *Loi pour la confiance dans l'économie numérique*, 21 juin 2004, *Loi relative aux communications électroniques et aux services de communication audiovisuelle*, 9 juillet 2004, *Loi n° 2006-64 relative à la lutte contre le terrorisme et comportant diverses dispositions relatives à la sécurité et aux contrôles frontaliers*, 23 janvier 2006, *Loi relative à la prévention de la délinquance*, 5 mars 2007, etc.

48 Royaume Uni, *An Act to make provision for securing computer material against unauthorised access or modification; and for connected purposes* (1990, c. 18) [Computer Misuse Act 1990]

und Abfangens von Daten », article 202c), l'escroquerie commise au moyen de la manipulation de données informatiques (« *Computerbetrug* », article 263a), la falsification d'enregistrements techniques (« *Fälschung technischer Aufzeichnungen* », article 268), la falsification de données pouvant servir de preuve (« *Fälschung beweiserheblicher Daten* », article 269), la tromperie par la falsification d'un traitement de données (« *Täuschung im Rechtsverkehr bei Datenverarbeitung* », article 270), la modification de données (« *Datenveränderung* », article 303a), la modification frauduleuse de données et le sabotage informatique (« *Computersabotage* », article 303b).

En France, la notion de « système de traitement automatisé des données » joue un rôle-pivot dans le dispositif mis en place par la loi *Godfrain* du 5 janvier 1988 aux articles 323-1 à 323-7 du Code pénal.[49] Autour de trois principaux types de comportements incriminés (accès ou maintien non autorisés dans un système informatique, atteinte au fonctionnement de système et atteinte aux données informatiques qui s'y trouvent), sont incriminées la fourniture sans motif légitime des instruments de ces infractions, l'association de malfaiteurs en vue de les commettre, la tentative et la complicité. La loi n°2014-1353 du 13 novembre 2014 a élargi cet arsenal coercitif dans le sens de la lutte contre le trafic de données personnelles, créant une nouvelle infraction, consistant en l'introduction frauduleuse de données dans un STAD, leur extraction, détention, reproduction, transmission, suppression ou modification frauduleuses. La loi n° 2015-912 du 24 juillet 2015 sur le renseignement a encore alourdi les amendes sanctionnant ces infractions : l'infraction caractérisée par l'accès ou le maintien dans un STAD est sanctionnée de 30.000 € à 60.000 € d'amende, celle encourue par l'individu entravant ou faussant un STAD de l'État est passé de 100.000 € à 300.000€.[50]

Malgré ces sanctions importantes, il a été fait reproche à ces infractions d'être trop déconnectées du préjudice réel engendré. Cette lacune pourrait être compensée par la possibilité de poursuivre de tels agissements parallèlement sur la base d'infractions liées au STAD et du vol.[51] Elle participe par ailleurs de la vision globale d'un législateur soucieux de lutter, au-delà du piratage, contre le trafic

49 Voir lexique, entrée **STAD**. Notons que le STAD n'est pas défini par la loi française et que la jurisprudence a opté pour une interprétation très large.

50 L'article 323-5 prévoit par ailleurs un certain nombre de peines complémentaires, incluant l'interdiction d'exercer l'activité professionnelle au cours de laquelle l'infraction a été commise, la confiscation des matériels ou des logiciels qui ont permis la réalisation de l'infraction, la confiscation du produit de l'infraction, etc. De façon intéressante, conformément à l'article 323-6, les personnes morales peuvent être déclarées pénalement responsables.

51 L'arrêt rendu le 20 mai 2015 par la Cour de cassation française a été l'occasion pour la doctrine de rappeler le cheminement réalisé depuis la création de ces infractions, qui s'étaient initialement révélées très insatisfaisantes (DAOUD Emmanuel et PERONNE Géralsine, *Cyberattaques : la lutte s'intensifie*, AJ Pénal 2015 p.396). Les auteurs ont souligné l'importance du champ couvert par ces infractions liées au STAD, notamment de-par leur autonomie, laquelle laisse entrevoir la possibilité d'un cumul.
L'arrêt du 20 mai 2015 en est une nouvelle illustration : une personne s'était introduite dans l'extranet d'une agence publique et avait récupéré des documents dont l'accès aurait normalement été protégé. L'accès frauduleux n'avait pu être retenu mais ça n'avait pas empêché la chambre criminelle de confirmer l'arrêt d'appel, lequel condamnait cet individu, à la fois pour maintien frauduleux dans un STAD et pour vol de documents informatiques.

de données : une pénalisation « précoce » de ces comportements est possible, en amont du préjudice.[5253]

Toutes ces définitions de la cybercriminalité concordent sur un point central : la protection de la donnée personnelle. La position du Royaume-Uni, notamment, a alimenté un débat sur l'opportunité de cette notion-pivot. Convient-il de réduire la définition juridique de la cybercriminalité au champ du système informatique, de la donnée personnelle ou de la vie privée ? Voilà qui affectera aussi les comportements dont la criminalisation est sujette à débats.

Section 3 : Le débat sur l'appartenance de certains comportements à la cybercriminalité

Au sein de la cybercriminalité, les préjudices internes aux jeux en ligne, récalcitrants au rattachement territorial, n'ont longtemps connu qu'une résolution interne à leur univers virtuel. La réparation des préjudices revenait à la société propriétaire du jeu tandis que les administrateurs déterminaient la sanction appropriée (le bannissement temporaire, la confiscation des biens, la rétrogradation d'un ou plusieurs niveaux ou la suppression de l'avatar et la clôture du compte.)[54]

Dans une affaire de 2012 qui a fait jurisprudence, deux *hackers* avaient utilisé des RATs[55] pour voler des objets virtuels dans le jeu en ligne *Diablo III*. Vu le montant des vols, la société propriétaire, *Blizzard Entertainment*, après avoir rendu leur équipement aux joueurs dépouillés, a fait appel à la justice américaine. Arrêtés par le FBI, les deux jeunes gens ont été condamnés en Californie et dans le Maryland des chefs d'accès illégal à un ordinateur. Comme les « victimes » n'avaient pas subi de préjudice, la justice a calculé le montant des réparations d'après les gains des deux cyberdélinquants, calculés selon le taux de la salle des ventes en ligne du jeu.[56]

Les mondes virtuels échappent par nature au règne des lois territoriales. Une première solution est d'étendre leur empire. Ce cas d'école venu d'outre-Atlantique doit nous amener à relativiser un tel

52 Il s'agit tout de même d'infractions intentionnelles : l'article 323-1 utilise l'adverbe « frauduleusement » et la jurisprudence confirme que l'agent doit avoir la conscience infractionnelle et la volonté infractionnelle pour que l'incrimination opère.
53 Dans le même esprit, le législateur a mis en place des obligations de lancer l'alerte en cas d'incidents de sécurité liés aux STAD et particulièrement aux données personnelles. L'article 34 bis de la loi n° 78-17 du 6 janvier 1978 oblige les fournisseurs de services de communications électroniques au public à notifier à la CNIL les violations de leurs mesures de protection des données à caractère personnel qu'ils traitent.
54 Voir lexique, entrées **Administrateur** et **Avatar**.
55 Voir lexique, entrée **RAT**.
56 HILL Kashmir, *Future crime – These two Diablo III players stole virtual armor and gold — and got prosecuted IRL*, 20 mai 2015, Fusion, [en ligne] (consulté le 20 août 2015) http://fusion.net/story/137157/two-diablo-iii-players-now-have-criminal-records-for-stealing-virtual-items-from-other-players/.

procédé : les pirates ont été condamnés pour avoir piraté le jeu, pas pour le vol virtuel.[57] Une autre solution est d'autoriser les sociétés qui se partagent ces réalités à s'autoréguler.[58]

Dans *Second Life*, par exemple, c'est *Linden Lab* qui détermine quelle part de la législation s'applique à ses avatars. Quant à sa réglementation financière, certains s'alarmaient de la croissance rapide du volume de ses échanges, alors que la dérégulation aurait permis toutes les fraudes et stratégies de blanchiment d'argent. Les jeux d'argent dégageaient de telles sommes à l'intérieur du jeu que le FBI avait lancé plusieurs descentes en ligne, jusqu'à ce que la société californienne décide finalement de se plier à la loi américaine, qui interdisait ces jeux d'argent depuis octobre 2006.

Cette décision abrupte, s'ajoutant aux rumeurs de chaînes de Ponzi, a poussé la principale banque de *Second Life*, *Ginko Financial*, à la faillite dès l'été 2007 : *Ginko* pratiquait des taux d'intérêt très élevés – près de 44 % annuels. Aucune régulation n'interdisait d'ailleurs de tels montages financiers. Il n'existait pas davantage d'encadrement des faillites. Les clients de *Ginko* ont été payés « au prix de la course », comme jadis les investisseurs du Canal de Panama.[59]

Après cette première crise financière interne, *Linden Lab* a été contraint de mettre en place une autorité financière virtuelle, suivant un schéma devenu maintenant classique. Comme *ebay*, *facebook*, *twitter*, *wikipedia* et la plupart des plaques-tournantes d'Internet avant lui, *Second Life* s'efforce d'adopter la politique, le règlement les plus compréhensifs possible.[60]

La situation juridique des jeux en ligne est intéressante pour deux raisons. D'abord, en pratique, ils appartiennent au tissu de l'économie numérique et peuvent perpétuer l'existence au sein de celle-ci de zones de non-droit où blanchir les gains illicites. Ensuite, ils illustrent l'importance pour la Justice de contrôler les opérateurs privés qui régulent ces mondes virtuels. Enfin, ils posent la question de la légitimité du législateur, du policier ou du juge à encadrer Internet. Dans bien des cas, sur la toile, l'État pourvoyeur de droit a cédé la place à l'entreprise, négociatrice de normes contractuelles. Or, la perception des autorités comme illégitimes est une constante dans le monde numérique et contribue à le rendre opaque. Le cybercriminel se cache souvent derrière l'esprit libertaire, et presque de désobéissance civile, d'Internet.

57 Pour une autre illustration, ce ne sont jamais les viols d'avatars qui sont punis mais, à la limite, parfois, comme en France, le harcèlement sexuel en ligne qu'ils traduisent.France, *Code pénal*, article 222-33.
58 FALLERY Bernard et RODHAIN Florence, *Fondements théoriques pour une régulation d'Internet : La légitimation faible et la réflexivité forte*, Systèmes d'information & management, Volume 15, mars 2010, pp. 41-70 [en ligne] (consulté le 20 août 2015) http://www.cairn.info/revue-systemes-d-information-et-management-2010-3-page-41.htm.
59 MASOUNAVE Annick, *Enquête Le système financier de Second Life*, Revue Banque, hors-série « Second Life », octobre 2007, pp. 11-16.
60 Ebay, Facebook, Twitter, Fondation Wikimedia, *Conditions d'utilisation* [en ligne] (consulté le 20 août 2015) http://pages.ebay.fr/help/sell/policies.html, https://www.facebook.com/legal/terms?locale=fr_FR, https://support.twitter.com/articles/75576-regles-de-twitter et https://wikimediafoundation.org/wiki/Terms_of_Use/fr.

Chapitre 3 : Le camouflage des réseaux de trafic de données personnelles dans l'univers des *hackers*

Le terme de « *hacker* » est universel mais la réalité qu'il recouvre est protéiforme et les activités du *hacker* ne se résume pas au trafic de données personnelles sur Internet (*section 1*). Le qualificatif s'étend au-delà de la délinquance informatique et se divise en catégories dans lesquelles les trafiquants ne s'insèrent que très grossièrement (*section 2*), vu leur degré extrême de spécialisation (*section 3*).

Section 1 : Le caractère anecdotique du trafic de données personnelles dans l'univers des *hackers*

Le cinéma a promu une certaine image des *hackers*,[61] qui semble être entrée dans le vocabulaire du profane. A en croire le dictionnaire Larousse, le terme désigne une « *personne qui, par jeu, goût du défi ou souci de notoriété, cherche à contourner les protections d'un logiciel, à s'introduire frauduleusement dans un système ou un réseau informatique.* »[62] Les programmeurs considèrent au contraire que ce mot traduit un goût pour l'analyse méthodique, et souvent empirique, de systèmes inconnus : le *hacker* chercherait à connaître un système pour le dépanner ou l'améliorer. Ces professionnels parlent plutôt de « *cracker* » pour désigner le pirate informatique.[63]

Les évolutions de la technologie entraînent toujours l'apparition d'individus « hors-la-loi », qu'ils soient de simples curieux ou des délinquants exploitant les failles des réseaux pour leur profit.[64] Par exemple, certains *phreakers*[65] étaient de jeunes curieux, intéressés par la toute dernière technologie. D'autres étaient des escrocs d'un nouveau genre, particulièrement habiles à cette discipline appelée « l'ingénierie sociale ».[66]

De même, aujourd'hui, les *green hats* utilisent l'informatique pour atteindre leurs fins mercenaires.

61 Le cinéma américain a donné le jour à de nombreux exemples de *hackers*, tels les personnages de David Lightman (*phreaker*) dans *War Games* ou de Matt Farrell (*hacker green hat*) dans *Die Hard 4 Retour en Enfer.*
62 Dictionnaire Larousse, entrée « hacker » [en ligne] (consulté le 20 août 2015) http://www.larousse.fr/dictionnaires/francais/hacker/38812?q=hacker#754734.
63 Voir lexique, entrée **Cracker**.
64 Voir lexique, entrée **Faille**.
65 Voir lexique, entrée **Phreakers**.
66 MITNICK Kevin, SIMON William, *The art of deception - Controlling the Human Element of Security*, Wiley Publishing Inc., Indianapolis, Indiana, États-Unis, 2002, 352 pp. et MITNICK Kevin, SIMON William, *The art of intrusion - The Real Stories Behind the Exploits of Hackers, Intruders & Deceivers*, Wiley Publishing Inc., Indianapolis, Indiana, États-Unis, 2005, 270 pp..

Parallèlement, les *grey hats*, cette immense majorité, pénètrent dans les systèmes sans y être autorisés mais sans être animés de mauvaises intentions. Ils sont motivés par la recherche de l'exploit informatique. Les *white hats*, professionnels de la sécurité informatique, arrivent simplement en remplacement des générations passées de consultants en sécurité et d'experts. Les trafiquants de données personnelles sont davantage des *green hats* que des *black hats*. En effet, par ce dernier terme, la plupart des pirates entendent désigner les *crashers*, qui violent la loi dans le seul but de détruire.

Vu le nombre de pirates informatiques, de nombreux sous-groupes ont fait leur apparition – *script kiddies*, codeurs, *elite hackers*, *phreakers*, *crackers*, *social engineers*, *blue hats*, *white hats*, *grey hats, black hats*, *green hats*, *crashers*, hacktivistes, *rippers*, *Nation States*, crime organisé, etc – nomenclature qui ne correspond pas très bien à la réalité des trafiquants de données personnelles.[67]

Section 2 : L'impossible insertion des trafiquants de données personnelles dans la nomenclature classique des *hackers*

Les *hackers* se distinguent les uns des autres selon plusieurs critères : leur compétence, leur insertion dans une organisation, leurs objectifs, leur souci de légalité ou leur médium de prédilection. Ces catégories sont anastomosées et ne recouvrent pas les trafiquants de données personnelles, dont la spécialisation rigidifie la nomenclature.

La compétence va naturellement fluctuer le long de la carrière des pirates, entre deux extrêmes : les *script kiddies*, néophytes empruntant leurs outils à de « vrais » *hackers*, et les *elite hackers*, qui sont au contraire les plus talentueux du lot. Les *script kiddies* sont susceptibles de causer des dommages considérables.[68]

Les trafiquants de données personnelles ne sont pas tous des codeurs, c'est-à-dire des pirates capables de créer leurs propres outils d'intrusion. Le vol de données personnelles ne requiert pas nécessairement des compétences techniques importantes. Alors que le travail en organisation facilite l'acquisition de compétences, le haut degré de spécialisation des trafiquants signifie qu'elle ne leur est pas indispensable.

À côté des groupes de trafiquants difficiles à mesurer, tel par exemple *Rex Mundi*, célèbre

67 Voir lexique, entrées **Black hat**, **Blue hat**, **Codeurs**, **Crime organisé (pirates du)**, **Elite hacker**, **Green hat**, **Grey hat**, **Hacktiviste**, **NS**, **Rippers**, **Script kiddies** et **White hat**.

68 Cette figure du monde numérique s'est dessinée suite aux exploits de Michael Calce. Ce Québécois de quinze ans a causé un préjudice inédit dans les années 2000, en lançant un certain nombre d'attaques par déni de service (voir lexique, entrée), et parmi les plus coûteuses.

pour son rançonnement des bases de données clients de grandes sociétés,[69] les réseaux de trafiquants de données sont généralement très structurés. Les organisations criminelles ont développé leurs activités au-delà de la simple institutionnalisation de la logistique informatique. Elles réaliseraient aujourd'hui 80 % des infractions commises sur Internet.[70] Les services de renseignement et les forces de l'ordre emploient aussi des légions de *hackers*, qu'ils revendiquent ou non leurs actions.[71]

Les *hackers* forment par ailleurs des alliances, qui leur sont utiles pour échanger des informations, et des groupes dont il est difficile de prendre la mesure ou de comprendre la nature. Les contours, par exemple, sont flous entre les groupes de *grey hats* et les groupes de *trolls* qui leur donnent le jour.[72] Les collectifs peuvent aussi s'institutionnaliser sous forme de firmes de sécurité.[73]

Plus ces groupes sont structurés, plus les objectifs de leurs membres seront déterminés par leur nature. Les groupes de trafiquants, eux, se sont structurés autour de leur objectif : l'appât du gain. La linéarité de ce propos explique leur pérennité supérieure à celle des collectifs *hacktivistes*. Les contours assez indéfinis de l'idéologie de ceux-ci (libertaire, antifasciste, altermondialiste, extrémiste religieux, etc) expliquent leur éclatement en courants.[74] Les objectifs des *grey hats* (la recherche de l'exploit), des *blue hats* et des *white hats* (la préservation du système et sa sécurité) leur permettent au contraire de travailler en autonomie et ne sont donc pas structurants.

Une certaine circonspection s'impose dans l'utilisation de ces termes, « *black hat* » et « *white hat* ». La distinction a été introduite par des *grey hats* sarcastiques tournant en ridicule le problème de la « légalité ». Elle renvoie à la dichotomie de l'imaginaire américain.[75]

69 Dernièrement, ce sont les données de sociétés médicales qu'ils rançonnaient : *Le collectif Rex Mundi a dérobé les données de 24.000 clients de la société AFC*, Sud Info, 20 juillet 2015 [en ligne] (consulté le 20 août 2015) http://www.sudinfo.be/1336319/article/2015-07-20/le-collectif-rex-mundi-a-derobe-les-donnees-de-24000-clients-de-la-societe-afc.

70 *La cybercriminalité coûte plus cher que les trafics de cocaïne, héroïne et marijuana*, Le Monde, 8 mai 2012 [en ligne] (consulté le 20 août 2015) http://www.lemonde.fr/technologies/article/2012/05/08/la-cybercriminalite-coute-plus-cher-que-les-trafics-de-cocaine-heroine-et-marijuana_1698207_651865.html.

71 L'Armée Electronique Syrienne (SEA), par exemple, un groupe de pirates informatiques créé au début de la guerre civile syrienne, en 2011, est responsable de nombreuses cyberattaques envers des médias occidentaux considérés comme hostiles à Bachar el-Assad (agences de presse, ONG, etc) : GUIBERT Nathalie, LELOUP Damien et UNTERSINGER Martin, *Comment « Le Monde » a été piraté par l'Armée électronique syrienne*, Le Monde, 20 janvier 2015 [en ligne] (consulté le 20 août 2015) http://www.lemonde.fr/pixels/article/2015/01/20/comment-le-monde-a-ete-pirate-par-l-armee-electronique-syrienne_4559393_4408996.html.

72 La *Gay Nigger Association of America*, par exemple, un groupe de *trolls* (voir lexique, entrée **Troll**) a donné le jour à *Goatse Security*, un groupe de *grey hats* spécialisé dans la révélation de failles de sécurité : LEWIS Helen, *Who are the trolls? - What we know about the men (and sometimes women) who spend their days trying to provoke a reaction on the internet*, New Statesman, 29 juillet 2013 [en ligne] (consulté le 20 août 2015) http://www.newstatesman.com/helen-lewis/2013/07/who-are-trolls.

73 Le collectif des *L0pht Heavy Industries* a été phagocyté par la société *Symantec* : TIMBERG Craig, *A disaster foretold, and ignored - LOpht's warnings about the Internet drew notice but little action*, The Washington Post, 22 juin 2015 [en ligne] (consulté le 20 août 2015) http://www.washingtonpost.com/sf/business/2015/06/22/net-of-insecurity-part-3/.

74 Voir, lexique, entrées **Antisec** et **Full disclosure**.

75 Dans une première version, il s'agirait de parodier les westerns classiques, où le héros porte un chapeau blanc et le méchant un chapeau noir. Les plus jeunes se réfèrent plutôt au *Seigneur des Anneaux*.

Il est difficile de déterminer quels pirates sont des *black hats*.[76] L'existence d'une victime ou d'un préjudice ne suffit pas. La communauté se réfère à trois critères : autorisation, motivation et intention, assimilant *black hats*, *crashers* et *green hats*. Elle peut donc réagir violemment aux plaintes de grandes entreprises contre les *grey hats*. Ainsi, lorsque *Sony* a poursuivi George Hotze, un *hacker* qui se déclare comme un *white hat*, qui lance des appels réguliers à ne pas révéler de données personnelles volées et qui a choisi de se tenir à l'écart du *jailbreak*[77] tant qu'il ne serait pas légal, les *Anonymous* ont lancé une attaque contre le groupe pour dénoncer l'injustice du procédé.[78]

À l'inverse, les trafiquants de données personnelles ne prétendent ni à la légalité, ni à la moralité.[79]

Section 3 : L'extrême spécialisation des trafiquants de données personnelles

Si les trafiquants de données personnelles cherchent à se distinguer les uns des autres, c'est uniquement d'après leurs spécialités respectives. La première d'entre elles sera le « *carding* », qui regroupe toutes les formes de fraude à la carte de débit et de crédit en ligne. Il y a aussi le *phishing* et le *pharming*, déjà évoqués ci-dessus, mais encore le *spamming*, ainsi que les activités menées par les *flèches* et par d'autres spécialistes.[80]

Le trafic de données se distingue du reste de la cybercriminalité par cette nomenclature fonctionnelle qui révèle l'existence de réseaux structurés et hiérarchisés de cyberdélinquants.[81] L'agent n'est pas lui-même versatile. C'est la multiplicité des talents coexistant au sein de la structure qui rend ces organisations efficaces. Leur ampleur leur permet de maintenir une pression par des attaques variées et nombreuses. Même si les autres *hackers*, fondamentalement

76 Un exemple typique est celui de Jon Lech Johansen (*DVD Jon*), un ancien *blue hat*, surtout connu pour son travail de décryptage des DVDs, qui lui a valu des poursuites en Norvège. Elles n'ont pas abouti, *DVD Jon* n'ayant pas en lui-même enfreint le droit d'auteur puisqu'il s'était contenté de décrypter les fichiers de DVDs qu'il possédait déjà.
77 Voir lexique, entrée **Jailbreak**.
78 KUSHNER David, *Machine Politics - The man who started the hacker wars*, The New Yorker, Annals of Technology, 7 mai 2012 [en ligne] (consulté le 20 août 2015) http://www.newyorker.com/magazine/2012/05/07/machine-politics.
79 Même Silk Road, un des sites les plus proéminents du Deep web, restreignait son activité à ce que le code éthique du site qualifiait de « *victimless contreband* » (« *une contrebande qui ne fasse pas de victimes* »), interdisant le trafic de pornographie, d'armes, de données personnelles ou de poisons : WESTIN Ken, *Stolen Target Credit Cards and the Black Market: How the Digital Underground Works*, The State of Security, 21 décembre 2013 [en ligne] (consulté le 20 août 2015) http://www.tripwire.com/state-of-security/vulnerability-management/how-stolen-target-credit-cards-are-used-on-the-black-market/ et GREENBERG Andy, *The Dark Web Gets Darker With Rise of the 'Evolution' Drug Market, Wired*, 18 septembre 2014 [en ligne] (consulté le 20 août 2015) http://www.wired.com/2014/09/dark-web-evolution/.
80 Voir, lexique, entrées **Carding** et **Smurfer**.
81 MATIGNON Emmanuelle, *La cybercriminalité: Un focus dans le monde des télécoms*, Mémoire Master Droit du numérique Administrations - Entreprises de l'École de droit de la Sorbonne (Université Paris 1 Panthéon-Sorbonne), année universitaire 2011/2012, 95 pp..

pragmatiques, peuvent se définir grossièrement par leur médium de prédilection, comme le *phreaker* (téléphone), le *cracker* (ordinateur) ou le *social engineer* (élément humain),[82] ils sont versatiles, ils doivent pouvoir diversifier leur approche pour réaliser les intrusions les plus efficaces.

Les ouvrages de référence du *hacking*, des manuels de sécurité informatique, *L'art de la persuasion* et *L'art de l'intrusion*, de Kevin Mitnick, expliquent d'ailleurs dans le détail, anecdotes à l'appui, comment combiner intrusion informatique et ingénierie sociale pour le mieux (voire *hacking*, *phreaking* et ingénierie sociale, tout à la fois).[83] Voilà l'une d'entre elles.[84]

Un jeune homme n'avait compris l'avantage d'entreprendre des études qu'à un âge où le retour à l'université était peu envisageable. Il se demanda comment, toutes lois et réglementations à part, se procurer un diplôme universitaire. Son nom était répandu dans la population américaine, il était probable que des homonymes aient été diplômés de l'université et dans le diplôme de son choix, au cours des années où il aurait pu l'être. Ce futur diplômé repéra l'URL[85] de l'intranet universitaire et se mit en quête des identifiants d'un administrateur. Il usa de ses connaissances en *phreaking* pour que son numéro semble provenir de l'enceinte de l'université et se fit passer pour un technicien informatique auprès du secrétariat de l'établissement. Il guida la secrétaire alors qu'elle tentait de se connecter au nouvel intranet, prétendument en cours de développement. En réalité, il s'agissait d'une fausse page de connexion qui avait transmis ses identifiants à notre jeune homme. Il la remercia, s'excusa au motif d'un problème informatique et raccrocha. Il n'avait plus qu'à se connecter, trouva deux homonymes, choisit celui dont l'âge était le plus proche du sien et s'appropria son diplôme.

À l'image de celle-ci, l'intrusion informatique est moins une affaire de technique que de capacité du *hacker* à varier son approche suivant les besoins de son plan. Ici, en utilisant un instrument à la portée de n'importe quel internaute, un individu a réussi à s'introduire dans le système informatique d'une université et à s'approprier les diplômes d'un autre. La force des trafiquants de données personnelles, au contraire, n'est pas leur capacité à s'introduire dans n'importe quelle cible mais le soutien d'une organisation capable de multiplier les attaques en empruntant à chaque fois la méthode de prédilection de la branche de l'organisation qui mènera l'assaut.

Leur niveau d'organisation ne suffit pourtant pas à les distinguer des autres pirates informatiques aux yeux de l'observateur extérieur. Outre ce camouflage, l'impunité des réseaux est

82 Voir lexique, entrée **Hacker**.
83 *The art of intrusion*, op. cit., p.72 : Une figure du piratage informatique et l'inventeur du *IP spoofing* (Voir lexique, entrée **IP spoofing**), Kevin Mitnick, dit *Condor*, était un si bon pirate qu'un procureur fédéral l'aurait accusé d'être « *capable d'obtenir le décollage des missiles intercontinentaux de l'Air Force rien qu'en sifflant dans le combiné d'un téléphone* » (« *A prosecutor once told a federal magistrate that if I was free to use a phone while in custody, I would be able to whistle into it and send instructions to an Air Force intercontinental missile.* »).
84 *The art of deception*, op. cit., pp. 124-128.
85 Voir lexique, entrée **URL**.

renforcée par le caractère immatériel et virtuel du web.

Titre II : Des difficultés liées à l'enquête, à la preuve et à l'exécution des décisions de justice

L'enquête, la condamnation et l'exécution des jugements sont particulièrement difficiles dans le cas de la cybercriminalité, faute de victimes coopératives (**Chapitre 1**), de moyens de preuve adaptés (**Chapitre 2**) et d'une vraie réponse au franchissement des frontières par le monde numérique (**Chapitre 3**).

Chapitre 1 : Des victimes discrètes, impliquant une démarche proactive des enquêteurs

Les forces de l'ordre ont été contraintes d'adopter une attitude proactive dans leurs enquêtes en matière de données personnelles, face à la rareté des plaintes (*section 3*). En effet, les entreprises amassant les données personnelles d'autrui déclarent rarement les vols dont elles sont victimes (*section 2*). Quant aux particuliers, bien que la protection de leurs données personnelles constitue leur principal sujet de préoccupation en matière numérique, ils prennent rarement les mesures qui pourraient les protéger ou leur permettraient d'être informés du vol qu'ils ont subi (*section 1*).

Section 1 : Le comportement ambigu des particuliers

La Commission européenne suit l'opinion publique des États membres depuis une quarantaine d'années, réalisant des sondages et créant des statistiques sur différents thèmes, dont la protection des données personnelles. Une dernière étude sur ce thème a été publiée en juin 2015.[86]

Au cours des dernières années, cet eurobaromètre a indiqué que les Européens se préoccupaient du sujet. Plus de la moitié d'entre eux évitent de communiquer leurs données personnelles en ligne (89 %), considèrent que le risque de devenir des victimes de la cybercriminalité augmente (85 %) ou s'inquiètent de ce que leurs données personnelles ne soient pas suffisamment protégées par les sites (73 %) ou par les administrations publiques (67%). La majorité d'entre eux prend des mesures pour se protéger dans ses activités en ligne (seuls 16 % se sont abstenus de prendre toute mesure).[87]

86 Commission Européenne, *Data protection Eurobarometer out today*, 24 juin 2015 [en ligne] (consulté le 20 août 2015) http://ec.europa.eu/justice/newsroom/data-protection/news/240615_en.htm.
87 Voir **Annexe 11 : Manifestations de l'inquiétude des populations de l'UE quant à la divulgation de données**

Cette prise de conscience est peu suivie d'effets. Les internautes de l'Union européenne se connectent de plus en plus – et pour des opérations très variées, incluant l'échange de messages électroniques (86% d'entre eux), la consultation des informations (63%), l'utilisation des réseaux sociaux (60%), leurs achats (57%), leurs opérations bancaires (54%), leurs jeux en ligne (29%), leurs ventes (23%) et la télévision en ligne (22%).[88]

Les eurobaromètres de 2013 et 2015 ne montrent pourtant pas d'évolution sensible dans le recours aux diverses parades envisageables pour la protection des données personnelles – installation d'un antivirus (parade utilisée par +5% des internautes de l'UE), limitation des échanges mails aux adresses connues (+3%), limitation de la publication de données personnelles en ligne (+3%), limitation du trafic Internet à des sites de confiance (+2%), utilisation exclusive de l'ordinateur personnel (+3%), utilisation de mots de passe différents (+11%), réduction des achats en ligne (+1%) et des opérations bancaires en ligne (aucune évolution). Les internautes semblent seulement prendre conscience de ce que le changement des paramètres de sécurité sur les services en ligne permet de protéger les données personnelles.[89]

La carte de l'eurobaromètre indiquant le niveau d'inquiétude, par pays, quant au manque de contrôle des internautes sur les données personnelles qu'ils communiquent en ligne, reflète bien un souci de protéger ces données mais, curieusement, les cartes indiquant quelles populations ont réagi par l'une des mesures évoquées ne correspondent pas.[90] Certaines populations, comme celle du Royaume-Uni, manifestent un grand souci des données personnelles, sans pour autant ressortir à l'une des solutions prescrites par les professionnels de la sécurité informatique. Paradoxalement, ces populations considèrent que la protection des données personnelles est l'affaire des sociétés privées (75 %) et celle de chaque individu (71%) bien avant d'être celle des autorités publiques (40%).

Ce fait devient particulièrement intéressant si l'on considère que les personnes privées sont celles qui inspirent le moins confiance aux internautes européens (entre 29 et 16 % des individus déclarent leur faire confiance contre 50 à 80 % pour les différentes autorités publiques). Les chiffres révèle que les Britanniques placent dans les opérateurs privés une confiance au-dessus de la moyenne.[91]

personnelles, **Annexe 12 : Réactions des populations de l'UE face à la crainte d'être victimes de cybermenaces** et **Annexe 13 : Carte de l'inquiétude des populations de l'UE quant à leur manque de contrôle sur les données personnelles qu'elles communiquent en ligne**.

88 Voir **Annexe 19 : Utilisation faite d'Internet par les populations de l'UE** et **Annexe 20 : Fonctions pour lesquelles Internet est utilisé dans l'UE**.

89 Voir **Annexe 14 : Carte : pourcentage des populations de l'UE qui ont installé un antivirus en réaction aux menaces informatiques**, **Annexe 15 : Carte : Européens qui changent leurs mots de passe en réaction aux menaces informatiques** et **Annexe 21 : Réactions des populations de l'UE à la crainte d'être victimes de cybermenaces**.

90 Voir **Annexe 13 : Carte de l'inquiétude des populations de l'UE quant à leur manque de contrôle sur les données personnelles qu'elles communiquent en ligne**.

91 Voir **Annexe 16 : Table de l'attribution de la responsabilité de la protection des données personnelles, de l'avis**

Cette différence, qui apparaît culturelle, pose la question du niveau de fiabilité des entreprises dans la collecte, le stockage et la gestion des données personnelles.

Section 2 : L'attitude peu protectrice des entreprises

Il faut noter que les sociétés en ligne à qui nous confions nos données personnelles ont tout intérêt à les protéger. C'est sur ce point que les rançonneurs du web comptent. Les informations qu'ils monnaient peuvent être objectivement de valeur, comme des données bancaires, ou elles peuvent n'en avoir que pour l'individu concerné. Récemment, par exemple, le site Internet *Ashley Madison*, qui propose des rencontres adultérines en ligne, a été massivement *hacké*. La rançon n'ayant pas été payée, des dizaines de millions d'identités ont été révélées en ligne.[92]

Non seulement il s'ensuit une perte de confiance des internautes, mais les piratages peuvent avoir de fâcheuses conséquences, économiques et judiciaires, pour le site ou l'application concernés.[93] Les entreprises évitent donc de médiatiser leurs fuites de données (à rebours de la volonté des peuples européens[94]) ou de rendre publics les vols de données personnelles dont elles sont informées,[95] et utilisent volontiers leurs modalités de traitement des données personnelles et leur transparence comme éléments de marketing.

Alors que les juridictions nationales peinent encore à admettre la nature de données personnelles des adresses *IP*, des fournisseurs de service Internet (FSI)[96] se sont mis à la même page que la CNIL et permettent à l'internaute de mesurer le pistage auquel il est soumis.[97] Ainsi, *Mozilla*

des populations de l'UE, par État membre et **Annexe 17 : Confiance des populations de l'UE dans les différentes autorités responsables de la collecte et du stockage des données personnelles**.

92 YADRON Danny, *Cyberattack could expose millions of users' personal information*, Wall Street Journal, 20 juillet 2015 [en ligne] (consulté le 20 août 2015) http://www.wsj.com/articles/affair-website-ashley-madison-hacked-1437402152 et Courrier International, 20 août 2015, Internet. Le piratage d'Ashley Madison révèle les limites de la vie privée en ligne [en ligne] (consulté le 20 août 2015) http://www.courrierinternational.com/article/internet-le-piratage-dashley-madison-revele-les-limites-de-la-vie-privee-en-ligne.

93 ELGOT Jessica, HERN Alex et WEAVER Matthew, *Ashley Madison adultery site hack: will I be found out?*, The Guardian, 21 juin 2015 [en ligne] (consulté le 20 août 2015) http://www.theguardian.com/world/2015/jul/21/ashley-madison-adultery-site-hack-will-i-be-found-out-what-you-need-to-know.

94 Voir **Annexe 22 : Positions sur la publicité des fuites de données personnelles**.

95 Les firmes de sécurité quadrillent sans cesse les marchés noirs virtuels pour compiler les données personnelles, surtout bancaires, volées et fournir ces listes aux banques mais celles-ci ne vont rendre l'information caduque en changeant les cartes bancaires que si l'opération est rentable. Il existe en effet un temps de latence entre la captation des données et leur utilisation frauduleuse et, plus la banque est importante, moins les pertes ponctuelles engendrées représentent un fardeau substantiel pour la banque, comparées au coût du remplacement systématique :
HACKETT Robert, *Why your bank may not care if your credit card was hacked*, Fortune, 26 juin 2015 [en ligne] (consulté le 20 août 2015) http://fortune.com/2015/06/26/bank-credit-card-hack/.

96 Voir lexique, entrée **Fournisseur d'accès Internet** et **Fournisseur de services Internet**.

97 Voir lexique, entrée **Cookie**.

Firefox, le fameux navigateur Internet,[98] propose une extension, *Lightbeam*, qui permet de visualiser le pistage de chaque internaute. L'image en annexe[99] illustre les activités de cette application, qui n'est que la grande sœur de *Cookieviz*, le logiciel traqueur de pistage proposé par la CNIL.[100]

Même les courtiers en données ont été obligés de faire preuve d'un certain degré de transparence. Une des plus grosses entreprises du domaine,[101] expérimente un site Internet qui donne aux internautes accès aux données recueillies sur leur compte ainsi qu'un droit de correction éventuel.[102]

Malgré ces louables efforts, les fuites de données personnelles n'ont jamais été si importantes. La simple diversité des attaques enregistrées est surprenante mais qu'il s'agisse de prises d'otages (*Ashley Madison*), de hold-ups (*Target*) ou de publications à des fins de disruption (*Sony*), la donnée personnelle est toujours au cœur de l'action de ces *hackers*.[103]

Cette tendance était en fait annoncée depuis longtemps par les spécialistes de la sécurité informatique. Ils constatent depuis des années une baisse du prix des données personnelles sur les marchés de la cybercriminalité et un changement de stratégie des *hackers*, qui cherchent à attirer plus de consommateurs en variant et en améliorant leurs services.[104][105] Les experts s'alarment de ce que les professionnels n'en tirent pas les conséquences en renouvelant leurs parades, par le passage de la lutte contre l'intrusion au cryptage[106] ou par une meilleure gestion des risques.[107][108][109]

Même à supposer que les entreprises parviennent à atteindre les plus hauts standards de protection des données personnelles, il est totalement impossible de prévenir leurs fuites et leur

98 Voir lexique, entrée **Navigateur Internet**.
99 Voir **Annexe 23 : L'application *lightbeam***.
100 Voir **Annexe 24 : La page de présentation de *Cookieviz*, l'application proposée par la CNIL**.
101 SINGER Natasha, *Mapping, and Sharing, the Consumer Genome*, The New Yorker, 16 juin 2012 [en ligne] (consulté le 20 août 2015) http://www.nytimes.com/2012/06/17/technology/acxiom-the-quiet-giant-of-consumer-database-marketing.html?_r=3&pagewanted=all.
102 HICKEN Melanie, *Find out what Big Data knows about you (it may be very wrong)*, CNN – Money, 5 septembre 2013 [en ligne] (consulté le 20 août 2015) http://money.cnn.com/2013/09/05/pf/acxiom-consumer-data/.
103 2014 a même été surnommée « *year of the data breach* » : NARAYAN Kaushik, *2014: The Year of the Data Breach – More Software Vulnerabilities and Breaches Than Any Year on Record*, Réseau Skyhigh, 2015 [en ligne] (consulté le 20 août 2015) https://www.skyhighnetworks.com/cloud-security-blog/2014-year-data-breach/.
104 JACKSON HIGGINS Kelly, *Glut In Stolen Identities Forces Price Cut In Cyberunderground*, Information Week, Dark Reading, 19 novembre 2013 [en ligne] (consulté le 20 août 2015) http://www.darkreading.com/attacks-breaches/glut-in-stolen-identities-forces-price-cut-in-cyberunderground/d/d-id/1140914.
105 Voir **Annexe 7 : Valeur des données personnelles *hackées*** et **Annexe 8 : Catalogue des marchés noirs de données personnelles**.
106 Voir lexique, entrée **Cryptage de données** et OHLHORST Frank, *Prevent 2015 from becoming another Year of the Data Breach*, TechRepublic, 11 décembre 2014 [en ligne] (consulté le 20 août 2015) http://www.techrepublic.com/article/prevent-2015-from-becoming-another-year-of-the-data-breach/.
107 OHLHORST Frank, *2015 prediction: Expect massive spikes in global information security threats*, TechRepublic, 19 novembre 2014 [en ligne] (consulté le 20 août 2015) http://www.techrepublic.com/article/2015-prediction-expect-massive-spikes-in-global-informationsecurity-threats/.
108 Département du Commerce, National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, 12 février 2014, 39 pp..
109 Voir lexique, entrée **Gestion des risques**.

utilisation frauduleuse. Une autre solution tient à la dissuasion. A charge pour les forces de l'ordre d'enquêter efficacement et d'appréhender les délinquants concernés.

Section 3 : La proactivité des forces de l'ordre

Face à l'ignorance ou au silence des victimes, les forces de l'ordre se voient contraintes d'adopter une attitude proactive contre la cybercriminalité. Pour intervenir avant l'acquisition frauduleuse des données personnelles, ils ont dû s'intéresser aux moyens de cette acquisition.

Parmi ces moyens, un des plus redoutables cible les particuliers : ce sont les *RAT*, programmes qui permettent de prendre le contrôle de l'ordinateur d'autrui. *DarkComet*, *BlackShades*, *Poisonivy*, etc, ils font trembler Internet et leurs développeurs s'enrichissent en les vendant sur le *deep web*.[110] Ils sont d'autant plus dangereux que même des pirates néophytes peuvent les utiliser pour accéder aux données d'autres internautes ou pour les enregistrer dans leur intimité. Chantages à la webcam, reventes de photos et de vidéos personnelles, détournements des données personnelles, transformations d'ordinateurs personnels en machines zombies s'ensuivent.

Les forces de l'ordre peuvent alors concentrer leurs efforts sur deux types de délinquants : les développeurs des différents *RATs* ou leurs clients, généralement des *script kiddies*. Il est plus facile d'appréhender les seconds, bien que l'arrestation de *hackers* néophytes soit généralement moins intéressante.

Les opérations en cascade arrivées à leur conclusion en mai 2014 et lancées à l'initiative du *FBI* avaient par exemple été rendues possibles par l'arrestation de co-développeurs du virus *BlackShades*, en 2012 et 2013. L'un d'entre eux, William Hogue, avait conservé les adresses *IP* de ses milliers d'acheteurs. Leur exploitation et le traçage des comptes *PayPal* utilisés pour le paiement des autres co-développeurs, ont permis de fermer deux noms de domaines[111] proposant *BlackShades* à la vente, d'exécuter plus de 350 perquisitions et 80 interpellations simultanées, en France, aux Pays-Bas, en Belgique, en Finlande, en Grande-Bretagne, au Danemark, au Canada et aux États-Unis.[112]

Ces mesures n'ont pas éradiqué le virus. Il continue de muter suite à la divulgation de son code. Il infecterait encore plusieurs centaines de milliers de machines. Inquiétant, si l'on considère l'ampleur

110 Voir lexique, entrée **Deep web**.
111 Voir lexique, entrée **Nom de domaine**.
112 EUDES Yves et SEELOW Soren, *Le logiciel espion Blackshades au cœur d'une grande enquête internationale*, Le Monde, 23 mai 2014 [en ligne] (consulté le 20 août 2015) http://www.lemonde.fr/societe/article/2014/05/23/le-logiciel-espion-blackshades-au-coeur-d-une-grande-enquete-internationale_4424783_3224.html.

du phénomène. En France seule, l'opération avait donné lieu à soixante-dix perquisitions et à une soixantaine de gardes-à-vue sur tout le territoire. Les gardés-à-vue auraient contrôlé une trentaine de webcams, dont ils revendaient l'accès, et auraient été en possession de plusieurs milliers de comptes *Paypal*, et *Facebook* piratés, sans parler des chantages à la webcam, des extorsions diverses et des données bancaires volées, qui servaient à la réalisation d'achats en masse.

L'arrestation de ces cyberdélinquants est encore compliquée par la difficulté d'établir des preuves dans le monde numérique. En effet, si celui-ci offre des possibilités nouvelles, les activités qui s'y déroulent et les propos qu'il sert le font entrer dans la sphère privée et justifient que la recherche de preuves s'entoure de certaines précautions.

Chapitre 2 : Une recherche de la preuve difficile dans le monde numérique

Les enquêteurs européens sont lourdement handicapés lorsqu'il s'agit de rassembler des éléments de preuve d'infractions numériques. Il leur faut faire intrusion dans une vie numérique qui ressort de la vie privée (*section 1*) et certains systèmes juridiques souffrent de rigidité pour développer de nouveaux types de preuves (*section 2*). Cette preuve essentiellement électronique n'est pas non plus sans se heurter à des obstacles techniques (*section 3*).

Section 1 : Le nécessaire encadrement par la loi de preuves pénales électroniques intrusives du point de vue des droits et libertés fondamentaux

Les États membres ont manifesté plus ou moins de rapidité et d'harmonie face à l'afflux de preuves électroniques. Certains, l'Espagne[113] et la Slovénie[114] par exemple, ont adopté des lois traitant du phénomène de façon globale.[115] D'autres, comme la Croatie, n'ont adopté leur code de procédure pénale qu'après l'apparition du phénomène.[116][117]

D'autres, enfin, faute d'avoir considéré le problème précocement et dans son ensemble, ont été contraints d'adopter des lois encadrant ponctuellement un mode de preuve ou un autre. Ainsi, en France, l'adoption d'une loi sur la géolocalisation a été nécessaire[118] après que la Cour Européenne des Droits de l'Homme (CEDH) a qualifié cette technique de recueil de la preuve d'intrusive et a réclamé son encadrement par une loi suffisamment claire et précise.[119]

Même à considérer que la preuve pénale soit libre, dans notre Union européenne gouvernée par les libertés et droits fondamentaux, elle devra toujours être encadrée par la loi lorsqu'elle

113 Espagne, *Ley 18/2011 reguladora del uso de las tecnologías de la información y la comunicación en la Administración de Justicia*, 5 juillet 2011 (*Loi 18/2011 régissant l'utilisation des technologies de l'information et de la communication dans l'administration de la justice*, 5 juillet 2011).
114 SELINŠEK Liljana, *Electronic evidence in the Slovene Criminal Procedure Act*, Digital Evidence and Electronic Signature Law Review, Volume 7, 2010, pp. 77-86.
115 URBANO CASTRILLO (de) Eduardo, *The legal regulation of electronic evidence: A pending necessity*, Digital Evidence and Electronic Signature Law Review, Volume 8, 2011, pp. 25-32.
116 Croatie, *Loi n° 71-05-03/1-08-2 portant adoption du code de procédure pénale*, 18 décembre 2008 (Journal Officiel de la République de Croatie n°152/2008).
117 SKRTIC Drazen, *Electronic evidence and the Croatian Criminal Procedure Act*, Digital Evidence and Electronic Signature Law Review, Volume 10, 2013, pp. 128-135.
118 Dalloz Actu Etudiant, 11 avril 2014, Focus sur, *La loi relative à la géolocalisation* [en ligne] (consulté le 20 août 2015) http://actu.dalloz-etudiant.fr.
119 VERGÈS Etienne, *Preuve pénale : la géolocalisation face à l'article 8 de la CEDH*, Revue des droits et libertés fondamentaux, RDLF, 2012, chronique n°04 [en ligne] (consulté le 20 août 2015) http://www.revuedlf.com/droit-penal/preuve-penale-la-geolocalisation-face-a-l%E2%80%99article-8-de-la-cedh/.

empiète sur la vie privée, ce qui risque de s'avérer fréquent. C'est l'exigence de légitimité de la preuve. La vie électronique est constituée en grande partie par des communications, lesquelles peuvent relever du champ de la vie privée.[120] En fait, dans le cas du *mail*, il peut aussi servir à identifier son expéditeur, devenant une donnée personnelle.[121]

Les particuliers ont fréquemment contesté l'enquête pénale au regard de l'article 8 de la Convention européenne des droits de l'Homme. En France, les juristes se souviennent bien du débat sur la sonorisation des pièces.[122] La CEDH n'a pas hésité à étendre à notre vie numérique le privilège d'une protection contre les enquêtes invasives.[123]

La procédure pénale a dû s'adapter à la nécessité de protéger les libertés fondamentales. En France, les actes d'enquête doivent respecter l'article 9 du Code civil instituant un droit général à la vie privée. Le recueil des preuves doit respecter la légalité et rentrer dans les exceptions aménagées par les règles procédurales. Ainsi, par exemple, l'article 432-9 du Code pénal réprime la violation du secret des correspondances en-dehors du contexte des articles 226-15 du Code pénal et 100 à 100-7 du Code de procédure pénale. Ces dispositions aménagent la possibilité pour un juge d'instruction d'ordonner l'interception de communications dans des enquêtes concernant des infractions passibles de peines d'emprisonnement égales ou supérieures à deux ans.[124]

Malgré le consensus entre pays démocratiques sur certains principes relatifs à l'enquête, les systèmes juridiques européens se sont adaptés différemment à la preuve électronique.

Section 2 : Les difficultés particulières des systèmes de *Common Law* face à l'arrivée de la preuve électronique dans le procès pénal

La valeur probante d'éléments électroniques fluctue parce que les règles d'admissibilité des preuves varient d'un système juridique à l'autre. Il en existe au moins trois dans l'UE : le système de *Common Law*, celui dit « de la loi nordique » et le système latin.[125]

120 CEDH, série A, Requête n° 269, 22 septembre 1993, *Klass c/ Allemagne* et CEDH, Requête n°59842/00, 30 mai 2005, *Vetter c/ France*.
121 Cour de première instance d'Athènes (Grèce), Ordre de paiement 1932/2011, 2011 (traduite et publiée dans Digital Evidence and Electronic Signature Law Review, Volume 10, 2013, pp. 198-200).
122 D'une cellule de prison, par exemple : CEDH, Requête n°71611/01, 20 décembre 2007, *Wisse c/ France*.
123 La saisie de données électroniques empiète sur la vie privée : CEDH, Requête n°74336/01, 16 octobre 2007, *Wieser et Bicos Beteiligungen Gmbh c/ Autriche*.
124 FÉRAL-SCHUHL Christiane, *Une procédure pénale adaptée à l'internet se dessine : entre « cyber-enquêteurs » et collaboration des fournisseurs et utilisateurs*, AJ Pénal, 2005, p. 228.
125 La loi nordique et la loi germanique sont souvent considérées comme des subdivisions des « *Civil law* », dont le système français est un autre exemple.

Ainsi, en France, la preuve pénale est libre. L'article 427 du Code de procédure pénale prévoit en effet que, « *hors les cas où la loi en dispose autrement, les infractions peuvent être établies par tout mode de preuve et le juge décide d'après son intime conviction.* » Au contraire, au Royaume-Uni, par exemple, la preuve est régie par des règles d'admissibilité strictes. Persistent des interdictions touchant au témoignage du conjoint, au ouï-dire (*hearsay*) et aux antécédents de l'accusé. Le juge a aussi le pouvoir d'écarter du débat les preuves pouvant avoir un effet préjudiciable sur l'esprit des jurés ou celles obtenues par violence ou déloyauté.[126]

Ces principes, de légitimité, de loyauté de la preuve, hormis des difficultés de l'ordre de l'épiphénomène,[127] font l'unanimité dans les pays démocratiques.

Les enquêteurs français, par exemple, sont tributaires du principe de loyauté de la preuve. Il faut noter que la Chambre criminelle de la Cour de cassation se montre plus ou moins exigeante suivant que la preuve est fournie par des autorités publiques ou par des sources privées.[128] Pour les secondes, la loyauté de la preuve prime sur le principe d'efficacité, le seuil se situant au niveau de la provocation à la commission d'une infraction par un agent public ou du stratagème. Cette limite affecte une méthode de recueil de preuve qui joue un rôle majeur sur Internet : l'infiltration, qui consiste « *à surveiller des personnes suspectées de commettre un crime ou un délit en se faisant passer, auprès de ces personnes, comme un de leurs coauteurs, complices ou receleurs* ».[129]

L'article 706-47-3 du Code de procédure pénale autorise les actes d'infiltration dans le domaine de la cybercriminalité mais seulement s'il existe des éléments antérieurs permettant de soupçonner l'existence d'infractions. Il ouvre même la porte à des « cyberpatrouilles », sous une forme strictement réglementée. À la différence de la provocation à l'infraction, la provocation à la preuve, c'est-à-dire l'intervention du policier qui n'a pas déterminé les agissements des personnes

126 HALPÉRIN Jean-Louis, *La preuve judiciaire et la liberté du juge*, Communications, Numéro 84, dirigé par Rafael Mandressi, « Figures de la preuve », 2009, pp. 21-32 [en ligne] (consulté le 20 août 2015) http://www.persee.fr/web/revues/home/prescript/article/comm_0588-8018_2008_num_84_1_2504.

127 La légitimité de la preuve implique que son recueil suive un procédé légal. La Cour de cassation belge, qui reconnaissait de longue date la preuve obtenue illégalement (Cass., 1985-86, n° 558, 13 mai 1986, *Arresten van het Hof van Cassatie*), est revenue sur ce principe depuis le début des années 2000 (Cass., 2003-04, n°814, 14 octobre 2003, *Rechtskundig Weekblad; Tijdschrift voor Strafrecht*). Au Royaume-Uni, par contre, on applique le principe du « fruit de l'arbre empoisonné », les preuves recueillies illégalement doivent toutes être exclues.

128 Cour de cassation, LEMOINE Pascal, Étude *La loyauté de la preuve (à travers quelques arrêts récents de la chambre criminelle)* [en ligne] (consulté le 20 août 2015) https://www.courdecassation.fr/publications_26/rapport_annuel_36/rapport_2004_173/deuxieme_partie_tudes_documents_176/tudes_diverses_179/travers_quelques_6401.html.

129 C'est ce type d'opération qui a permis d'appréhender le créateur de l'immense marché noir en ligne connu sous le nom de « *Silk Road* ». Suite à l'arrestation d'un de ses employés, un agent du FBI lui avait proposé ses services de tueur à gage. Le pirate connu sous le nom de « Dread Pirate Roberts » l'avait engagé pour exécuter son complice avant qu'il ne puisse collaborer avec la Justice : JEONG Sarah, *The DHS Agent Who Infiltrated Silk Road to Take Down Its Kingpin*, Forbes, 15 janvier 2015 [en ligne] (consulté le 20 août 2015) http://www.forbes.com/sites/sarahjeong/2015/01/14/the-dhs-agent-who-infiltrated-silk-road-to-take-down-its-kingpin/.

suspectées, est autorisée.[130] Il s'agit seulement de constater l'infraction.[131]

Le Code de procédure pénale permet d'autres formes de recueil de preuves : la réquisition informatique (article 60-2, alinéa 1), la préservation des contenus (article 60-2, alinéa 2), l'interception des données (articles 100 à 100-7), la perquisition et la saisie de données informatiques (article 56 alinéa 5), la géolocalisation (articles 230-32 à 230-44) ou encore l'envoi d'un cheval de Troie (article 706-102-1 à 206-102-9).[132] Toutes ces mesures sont soumises à l'autorisation du juge des libertés et de la détention.[133]

Dans les pays de *Common Law*, l'adaptation a été plus difficile, vue la rigidité des modes de preuve. Un problème a été de déterminer qui était le témoin « compétent ». Au Royaume-Uni, seul le témoin compétent peut témoigner. En droit britannique,[134] la compétence est la capacité à comprendre toutes les questions portant sur les faits ou sur les éléments de preuve matériels et à y répondre. La formation d'experts en informatique assez compétents a pu être longue, l'utilisateur d'un outil informatique n'étant pas forcément un expert de son maniement.[135]

La règle de la meilleure preuve, ou de la preuve de source primaire, impose aussi d'utiliser comme preuve l'élément qui offre la meilleure qualité ou qui se rapproche le plus de l'original. Il s'agissait de réduire les risques de mauvaise transcription ou de modification frauduleuse, à l'origine, mais même l'interprétation stricte de cette règle autorisait les copies lorsque l'original était perdu ou inaccessible. Elle s'est encore assouplie pour s'adapter à la révolution numérique.

La preuve par ouï-dire est également interdite, c'est-à-dire la preuve donnée par un témoin au sujet d'une déclaration d'une personne absente du tribunal. Cette règle a été abolie au civil dans les années 90.[136] Elle persiste au pénal et pourrait recouvrir toutes les preuves numériques concernant la déclaration d'une personne absente. La doctrine ne partage pas cet avis.[137] Les exigences de transparence du recueil et de pertinence de tous les éléments de preuve produits lors du procès pénal sont enfin très difficiles à atteindre dans le cas de la preuve électronique.[138]

130 Cass. Crim. (France), n° 97-85.747, 30 avr.il 1998 (Bull. crim. n°147), Cass. Crim. (France), n° 05-82.012, 8 juin 2005 (Bull. crim. n°173), Cass. Crim. (France), n° 07-87.633, 16 janvier 2008 (Bull. crim. n° 14).
131 *Protéger les internautes – Rapport sur la cybercriminalité*, op. cit., « Les réponses actuelles à la cybercriminalité en France : de l'appréhension normative à la spécialisation de la police judiciaire pour une efficacité relative », pp. 33-46.
132 Voir lexique, entrée **Cheval de Troie**.
133 Myriam QUÉMÉNER, *Les spécificités juridiques de la preuve numérique*, AJ Pénal, 2014, p. 63.
134 Royaume-Uni, *Youth Justice and Criminal Evidence Act*, 1999 (YJCEA 1999), section 53.
135 *A framework for a syllabus on electronic evidence*, Digital Evidence and Electronic Signature Law Review, Volume 10, 2013, pp. 7-15 et ITU, Secteur du développement des télécommunications, *Comprendre la cybercriminalité – Phénomène, difficultés et réponses juridiques*, Genève, septembre 2012, p. 241.
136 Royaume-Uni, *Civil Evidence Act*, 8 novembre 1995 (1995 c. 38).
137 GALVES Fred, *Where the not-so-wild things are: Computers in the Courtroom, the Federal Rules of Evidence, and the Need for Institutional Reform and More Judicial Acceptance*, Harvard Journal of Law & Technology, Volume 13, n°2, 2000, p. 246.
138 *Comprendre la cybercriminalité – Phénomène, difficultés et réponses juridiques*, op. cit., « Recevabilité des

Malgré les difficultés techniques et juridiques, les enquêteurs de l'Union européenne ont été contraints de recourir à des moyens de preuve novateurs, ce qu'annonçait déjà, au début des années 2000, le rapport explicatif de la Convention sur la cybercriminalité du Conseil de l'Europe.[139]

Section 3 : La difficulté technique de recueillir des preuves dans le monde numérique

Les policiers ont tenté de retourner leurs propres outils contre les *hackers*. Comme ces derniers recueillent les données personnelles d'internautes avec discrétion et efficacité, les enquêteurs ont envisagé d'acquérir efficacement et discrètement des preuves sur les systèmes informatiques, réseaux ou machines, que les pirates informatiques utilisent.

Il leur fallait surmonter un ensemble d'obstacles : les *hackers* ne sont pas des cibles naïves et vulnérables, mais au contraire très prudentes, ils savent dissimuler ou chiffrer leurs données, sont prompts à les détruire. Ils sont aussi mobiles et recourent autant que possible à l'anonymat. Ils connaissent les instruments d'intrusion et peuvent les détourner ou les abuser. Les enquêteurs doivent, lorsqu'ils créent leurs propres outils, s'assurer que ceux-ci ne puissent être détectés, qu'ils puissent être utilisés et réutilisés, et qu'ils soient efficaces. Les expériences ont montré que les fausses alertes devaient être évitées à tout prix.[140] Il ne faut pas davantage que ces logiciels puissent être détournés. Les virus enquêteurs peuvent nuire à la sécurité des ordinateurs dans lesquels ils sont installés.[141]

Plusieurs logiciels de ce type se sont illustrés dans la presse. Carnivore, par exemple, réalise des interruptions de communications électroniques. Le FBI a aussi utilisé le ver espion *Magic Lantern* dans les années 90 pour récupérer des mots de passe et clés de chiffrement.[142] Un autre virus, *DIRT*, a inspiré nombre de romans d'espionnage, avec sa capacité d'enregistrement de la frappe.

Plus significatif sans doute, des dispositions sont apparues, qui prévoient l'introduction des preuves

preuves numériques », pp. 244-247.

139 Conseil de l'Europe, Rapport explicatif sur la Convention sur la cybercriminalité, STE n° 185, 8 novembre 2001 [en ligne] (consulté le 21 août 2015) http://conventions.coe.int/Treaty/FR/Reports/Html/185.htm.

140 Pedoworm est un exemple particulièrement frappant. Pour la première fois repéré dans les années 2000, cet outil avait été inventé par des *hackers* pour dénoncer les pédophiles aux forces de l'ordre. Il infectait les ordinateurs par l'échange de courriers électroniques. Il fouillait leurs disques durs à la recherche de fichiers images à contenu potentiellement pédophile. Il était d'une rare inefficacité, lançant sans cesse des fausses alertes et ayant un impact désastreux sur les machines infectées. Il ne surmontait pas le plus petit effort de cryptage ou de dissimulation.

141 Sony s'est mis en difficulté au début des années 2000, lorsqu'il s'est avéré que les *rootkits* (Voir lexique, entrée **Rootkit**) qu'installaient ses CDs facilitaient le piratage des machines.

142 Voir lexique, entrée **Ver**.

ainsi obtenues dans la procédure pénale. Ainsi, par exemple, la doctrine n'a guère réagi à l'apparition des virus enquêteurs dans la loi pénale portugaise, en 2009.[143]

Le fait que les logiciels médiatisés aient tous été créés et utilisés au début des années 2000 suggère que les forces de l'ordre utilisent à présent des virus difficiles à détecter.[144]

Les législateurs européens se sont aussi adaptés aux réalités du stockage des données. La perquisition électronique, au début pensée comme une extension de la perquisition physique, a été autorisée à suivre les données, de proche en proche. L'enquêteur peut accéder et saisir les données placées dans le *cloud*, notamment, ou sur des serveurs à l'étranger.[145][146][147]

Cette délocalisation complique l'établissement de la preuve[148] mais le principal problème de l'enquêteur reste le talent des pirates pour couvrir leurs traces. Ils exploitent ainsi des techniques de dissimulation des données[149] et de cryptage. Le législateur slovène a trouvé une parade intéressante : l'article 219.a.6 du Code de procédure pénale slovène impose au propriétaire ou à l'utilisateur d'une machine d'en autoriser l'accès aux forces de police (fournir clés et mots de passe de décryptage), le manquement à cette obligation constituant une infraction.[150]

Les pirates tiennent le juriste en échec par des parades plus sournoises encore. La défense par le cheval de Troie a fait des ravages en Slovénie. Le sujet de l'enquête conteste les preuves informatiques en prétendant qu'elles ont été manufacturées par le biais d'un logiciel malveillant. Cette défense, si elle est étayée par quelques commencements de preuve, implique que les preuves électroniques ne suffisent pas et doivent être accompagnées d'un commencement de preuve matérielle.[151]

143 SILVA RAMALHO David, *The use of malware as a means of obtaining evidence in Portuguese criminal proceedings*, Digital Evidence and Electronic Signature Law Review, Volume 11, 2014, pp. 55-75.
144 FILIOL Éric, *Notes sur les méthodes techniques d'acquisition de la preuve Virus et vers « enquêteurs »*, Séminaire « Criminalité en Europe », Laboratoire de virologie et de cryptologie, École Supérieure et d'Application des Transmissions (ESAT), 5 juillet 2007, 14 pp..
145 Voir lexique, entrées **Cloud computing** et **Serveur Internet**.
146 VACIAGO Giuseppe, *Remote forensics and cloud computing: an italian and european legal overview*, Digital Evidence and Electronic Signature Law Review, Volume 8, 2011, pp. 126-129.
147 BAGBY John et SCHWERHA Joseph, *International aspects of migrating digital forensics in the cloud*, Digital Evidence and Electronic Signature Law Review, Volume 10, 2013, pp. 81-96.
148 Conseil de l'Europe, Comité de la Convention sur la cybercriminalité, Groupe sur les preuves dans le nuage, *Défis de l'accès de la justice pénale aux données stockées dans le nuage*, Document de réflexion T-CY (2015)10, Strasbourg (France), 26 mai 2015, 25 pp. [en ligne] (consulté le 20 août 2015)
https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016803053cb.
149 ILIOUDIS Christos, MARTINI Adamantini, RACHAVELIAS Michael et ZAHARIS Alexandros, *Hiding illegal content in the swf format and spreading through social network services: a legal approach*, Digital Evidence and Electronic Signature Law Review, Volume 7, 2010, pp. 117-121.
150 ŠEPEC Miha, *Digital data encryption – aspects of criminal law and dilemmas in Slovenia*, Digital Evidence and Electronic Signature Law Review, Volume 10, 2013, pp. 147-154.
151 ŠEPEC Miha, *The trojan horse defence – a modern problem of digital evidence*, Digital Evidence and Electronic Signature Law Review, Volume 9, 2012, pp. 58-66.

A cette fragilité de la preuve électronique, s'ajoute une impossibilité pour l'enquêteur d'accéder à certaines données. Il lui faut pour en avoir connaissance obtenir l'assistance d'opérateurs privés, fournisseurs de services Internet (FSI) ou fournisseurs d'accès Internet (FAI), ce qui n'est envisageable que dans la mesure où ils appartiennent au champ de la compétence des juridictions auxquelles il peut s'adresser.

Chapitre 3 : Une criminalité se jouant des frontières

La cybercriminalité se déroule dans un monde virtuel, donc transfrontalier. Nos tribunaux doivent par conséquent procéder à un découpage des juridictions déterritorialisé (*section 1*). L'extradition des criminels et l'exécution des jugements étrangers ont aussi dû être facilités (*section 2*).

Section 1 : Le problème de l'extranéité

Le réseau Internet dépasse les frontières au point que certains auteurs le traitent en espace international, au même titre que la lune et les corps célestes ou que les océans, qui sont des environnements régis par la voie conventionnelle.[152] Or, la loi pénale est par nature territoriale. La cybercriminalité apporte dans l'immense majorité des cas un élément d'extranéité.

Le cyberespace n'est pas pour autant une zone de non-droit.[153] Il existe plusieurs facteurs de rattachement aux droits nationaux. La France retient le lieu de commission des faits, la nationalité de leur auteur et celle de la victime.

Quant au rattachement par le lieu de commission des faits, l'article 113-2 prévoit que la loi pénale française s'applique aux infractions commises sur le territoire. L'infraction est réputée telle dès que l'un de ses faits constitutifs a eu lieu sur ce territoire. Un exemple de fait constitutif peut être l'orientation vers un public français lorsque les serveurs sont localisés à l'étranger.[154] Quand l'infraction a été commise à l'étranger, l'article 113-5 du Code pénal impose une condition de double incrimination pour que la loi pénale française s'applique aux complices de cette infraction ayant agi en France.

Quant au rattachement par la nationalité de l'auteur, si les infractions ont été commises en dehors du territoire national, l'article 113-6 du Code pénal distingue entre les crimes et les délits. La loi pénale française est applicable à tout crime commis par un français hors du territoire national. En revanche, elle n'est applicable aux auteurs de délits que si les faits sont punis par la législation du pays où ils ont été commis – condition de double incrimination qui concerne surtout les **délits** informatiques.

152 BÉNICHOU David, *Cybercriminalité : jouer d'un nouvel espace sans frontière*, AJ Pénal, 2005, p. 224.
153 Voir lexique, entrée **Cyberespace**.
154 TISSIER Guillaume (dir.), Étude *Les marches noirs de la cybercriminalité*, Compagnie Européenne d'Intelligence Stratégique (CEIS), Collection Notes Stratégiques, Technologies de l'information, équipe Secu-Insight de CEIS, juin 2011, pp. 56-60.

Quant à la nationalité de la victime, l'article 113-7 du Code pénal dispose que la loi pénale française est applicable à tout crime et à tout délit puni d'emprisonnement commis par un Français ou par un étranger hors du territoire de la République, lorsque la victime est de nationalité française au moment de l'infraction. Les effets de cette disposition ont été étendus aux cas où une convention internationale donne une compétence à la France.

Notons par ailleurs qu'en matière de responsabilité délictuelle, l'article 46 du Code de procédure civile donne le choix au demandeur entre la juridiction du lieu où demeure le défendeur, celle du lieu du fait dommageable et celle dans le ressort duquel le dommage a été subi.[155]

La territorialité de la loi pénale importe aussi pour le recueil des preuves. En effet, pour obtenir des opérateurs privés du monde informatique qu'ils coopèrent, il faut les placer sous l'empire d'une juridiction nationale. Un débat sur la question a d'ailleurs opposé l'opérateur *Yahoo!* et les juridictions belges. Le législateur belge fait obligation aux opérateurs privés de coopérer avec le Ministère public dès lors qu'ils ont une présence électronique sur le territoire national, c'est-à-dire, en l'occurrence, dès lors qu'une société offre des services de communication électronique sur le territoire et peut être jointe depuis ce territoire. Le FSI considère que, n'ayant pas de présence locale matérielle, il ne ressort pas de la compétence belge. Il y a eu une série de décisions *Yahoo!*, sans que la société de droit californien se plie aux exigences du procureur belge.[156]

Le débat semble opposer l'Europe et l'Amérique. La Cour de justice de l'Union européenne (CJUE) impose des conditions assez larges pour établir sa compétence sur les activités d'une société de droit américain. Dans son récent arrêt sur le droit à l'oubli, la juridiction européenne a considéré que les règles de l'UE s'appliquent à un moteur de recherche dont les serveurs sont localisés hors d'Europe s'il a une branche ou une succursale dans ses frontières qui promeut la vente d'espace publicitaire sur le FSI.[157] Le dispositif juridique européen de lutte contre la cybercriminalité repose sur la capacité des décisions européennes à s'appliquer sur le territoire de juridictions étrangères.

Section 2 : Les difficultés en matière d'extradition et d'exécution des jugements

Les opérateurs privés détiennent les clés d'Internet. Ils interviennent au stade de la collecte

155 PADOVA Yann, *Un aperçu de la lutte contre la cybercriminalité en France*, RSC, 2002, p. 765.
156 VANDENDRIESSCHE Johan, *The effect of 'virtual presence' in Belgium on the duty to cooperate with criminal investigations: some prudence may be required when confronted with a request from a Belgian public prosecutor*, Digital Evidence and Electronic Signature Law Review, Volume 8, 2011, pp. 194-195.
157 CJUE, Affaire C-131/12, 13 mai 2014, *Google Spain SL et Google Inc. contre Agencia Española de Protección de Datos (AEPD) et Mario Costeja González*.

des preuves, par exemple en offrant des canaux de signalement.[158] Ils jouent aussi un rôle dans l'exécution des décisions. La Justice ne pourrait pas assainir l'environnement numérique sans la coopération des FSI. C'est la coopération de ces opérateurs qui permet de bloquer l'accès aux marchés noirs de la cybercriminalité et aux contenus illégaux sur Internet.

Les acteurs privés jouent aussi un rôle majeur de formation des enquêteurs, particulièrement dans les États de *Common Law* où le recours à la société civile fait partie de la culture judiciaire. Ainsi, au Royaume-Uni, les opérateurs Internet sont réunis au sein de l'*Internet Watch Foundation*, dont la mission principale est la lutte contre la diffusion de contenus pornographiques sur Internet.[159] Interpol l'a rappelé à l'occasion d'une récente opération internationale visant à mettre le virus *Simda* hors d'état de nuire avec le concours de *Microsoft* et d'autres opérateurs, la plus grande partie de l'expertise informatique se trouve dans le secteur privé, il faut donc encourager les partenariats.[160]

Cette participation est d'un intérêt moindre lorsque l'opérateur ne l'offre pas librement. La Chine, par exemple, dont la législation est extrêmement dure en matière de cybercriminalité, incluant depuis le début des années 2000 un contrôle à priori des contenus Internet, est encore une des sources les plus abondantes de cybercriminalité.[161] Le contrôle strict des FSI ne paraît pas à même d'engendrer les résultats désirés.

Par ailleurs, dans nos États occidentaux, s'il existe une forme de responsabilité du fournisseur qui ne prend pas des mesures minimales de lutte contre la cybercriminalité (en limitant l'accès, en transmettant l'information à la police), face à un conflit de lois ou de valeurs, l'opérateur optera pour l'ordre juridique qui l'avantagera le plus.

Le cas le plus connu est peut-être celui qui a opposé la ligue contre le racisme et l'antisémitisme (LICRA) et l'Union des étudiants juifs de France (UEJF) à la société californienne *Yahoo*!. L'entreprise permettait la vente d'objets nazis sur son site de vente aux enchères. Une juridiction française avait délivré des injonctions aux fins de faire retirer cette vente du site ou de filtrer l'accès des internautes français. *Yahoo!* s'était opposé devant un tribunal californien à l'exécution de cette décision et la juridiction américaine l'avait refusée au jugement français, au nom de la liberté

158 FÉRAL-SCHUHL Christiane, op. cit..
159 Internet Watch Foundation (IWF), *Remit, Vision and Mission* [en ligne] (consulté le 20 août 2015) https://www.iwf.org.uk/about-iwf/remit-vision-and-mission.
160 « *Le succès de cette opération démontre l'utilité et la nécessité des partenariats entre les services chargés de l'application de la loi, aux niveaux national et international, et les entreprises privées pour lutter contre la menace mondiale que constitue la cybercriminalité.* » : Interpol, *INTERPOL coordonne une opération mondiale visant à mettre le botnet Simda hors d'état de nuire*, Singapour, 13 avril 2015 [en ligne] (consulté le 20 août 2015) http://www.interpol.int/fr/Centre-des-médias/Nouvelles/2015/N2015-038.
161 Sur la dernière mesure chinoise de lutte contre la cybercriminalité, qui semble avoir surtout permis l'arrestation d'opposants politiques : Cour Suprême populaire, « *China internet police to "come to the frontstage": Ministry* », 2 juin 2015 [en ligne] (consulté le 27 septembre 2015) http://en.chinacourt.org/public/detail.php?id=4982.

d'expression, estimant qu'il aurait été contraire à l'ordre public californien d'exécuter une telle décision.[162]

Les juridictions sont moins réticentes à l'extradition, qui apparaît pourtant d'une nature plus sensible. Des extraditions se sont révélées impossibles, mais ces dysfonctionnements restent rares entre les États membres et leurs partenaires les plus engagés contre la cybercriminalité. L'existence du mandat d'arrêt européen (MAE) a par ailleurs facilité la remise des criminels.

En général, les obstacles à l'extradition ou à la remise sont de nature politique. L'affaire Julian Assange serait un de ces cas.[163] Le MAE lancé par la Suède contre le *hacker* à l'origine de *Wikileaks* n'a en effet pas été suivi d'effets car le pirate s'est réfugié dans l'ambassade de l'Équateur à Londres. C'est le pays sud-américain qui s'oppose à l'extradition car Assange, recherché dans l'UE pour une affaire de viol et d'agression sexuelle, risquerait d'être extradé vers les États-Unis à cause de ses activités de *hacker*.[164]

La coopération judiciaire au sein de l'Union a évolué au-delà de l'extradition classique, en dotant les États membres d'un cadre qui harmonise et rationalise les garanties accordées dans le cadre de la remise.[165] Les criminels condamnés semblent en tout cas maîtriser les manœuvres dilatoires rendues possibles dans le droit des États membres de l'UE.[166] Dans les États où les garanties accordées dépendent du bon vouloir des autorités nationales, comme la Russie ou l'Équateur, l'extradition tend à se transformer en bras-de-fer politique et c'est plutôt la recherche des cybercriminels qui s'est avérée compliquée. Le Congrès américain propose depuis 2013 une solution originale, le Programme de primes pour le crime organisé transnational. Parmi les huit primes offertes, sept concernent des criminels qui se trouveraient dans les sphères d'influence chinoise et russe, et le dernier dans l'Union européenne (*hacker* roumain).[167]

162 TGI Paris (France), 20 novembre 2000, *Ligue internationale contre le racisme et l'antisémitisme (LICRA) et Union des étudiants juifs de France (UJF) contre Yahoo!* et Cour suprême des États-Unis, 30 mai 2006.
163 *WikiLeaks la Grande-Bretagne refuse que Julian Assange quitte son territoire*, Le Monde, 16 août 2012 et *L'Elysée rejette la demande d'asile de Julian Assange*, 3 juillet 2015 [en ligne] (consultés le 20 août 2015) http://www.lemonde.fr/technologies/article/2012/08/16/la-grande-bretagne-determinee-a-extrader-julian-assange_1746459_651865.html#v1Ob5YMwL0g7gTar.99 et http://www.lemonde.fr/pixels/article/2015/07/03/l-elysee-rejette-la-demande-d-asile-de-julian-assange_4669082_4408996.html#CDErkX3H0wjA6Mkf.99.
164 Ce n'est donc pas à proprement parler un MAE dans le domaine de la cybercriminalité.
165 D'ailleurs, les États membres de l'Union européenne collaborent dans le cadre de « remises », et non d'« extraditions ». Dans le cadre classique, les possibilités d'extradition sont très limitées : les États n'extradent pas leurs nationaux, l'extradition est soumise à une condition de double incrimination et à l'accord des deux États concernés, délivré conformément à leurs procédures respectives.
166 En février dernier, par exemple, les Pays-Bas ont finalement extradé un Russe recherché pour avoir piraté des systèmes de paiement en ligne vers les États-Unis après l'avoir laissé contesté son extradition pendant plus de deux années (États-Unis, Département de la Justice, Bureau des affaires publiques, *Russian National Charged in Largest Known Data Breach Prosecution Extradited to United States*, 17 février 2015 [en ligne] (consulté le 20 août 2015) http://www.justice.gov/opa/pr/russian-national-charged-largest-known-data-breach-prosecution-extradited-united-states).
167 États-Unis, Département d'État, *Programme de primes contre le crime organisé transnational* (*Transnational Organized Crime Rewards Program*) [en ligne] (consulté le 20 août 2015) http://www.state.gov/j/inl/tocrewards/.

En conclusion, entre les États membres de l'Union européenne, les problèmes qui persistent, aux stades de l'enquête, du procès et de l'exécution de la peine, tiennent d'abord à une incohérence de la définition du phénomène cybercriminel ou de l'objet « données personnelles ». Deux polémiques coexistent. L'une vient d'une doctrine critique de la réduction de la cybercriminalité à un petit ensemble d'infractions tournant autour de la notion de donnée, mais qui ne souhaite pas davantage transformer la cybercriminalité en une notion éclatée et illisible. Tout un champ de comportements peuvent en effet être incriminés dans le cadre du phénomène de cybercriminalité, allant de l'acquisition irrégulière des données personnelles à leur utilisation frauduleuse. Vient ensuite la question de la donnée personnelle elle-même. Là encore, une définition restrictive s'oppose à une définition large, suivant que l'on considère ou non les informations qui ne sont ni biographiques ni liées à la vie privée.

À supposer que les infractions de l'arsenal législatif suffisent, les enquêteurs doivent encore adopter une démarche proactive : les victimes, qui sont généralement ignorantes ou discrètes, ne déclenchent pas l'enquête en déposant des plaintes. Les enquêteurs ont ensuite dû surmonter des obstacles avant de pouvoir recueillir des preuves des comportements cybercriminels. En effet, pour les pays du système juridique latin, il a fallu que le législateur encadre les moyens du recueil de la preuve 2.0. Quant aux systèmes anglo-saxons, c'est la rigidité du mode de preuve qui a posé problème. Enfin, les législateurs et les juridictions ont dû offrir des solutions permettant à des lois d'appréhender ce territoire virtuel qu'est Internet mais l'exécution des décisions de justice reste tributaire de la bonne volonté des opérateurs privés du web.

Partie II : Les spécificités financières du trafic de données personnelles sur Internet

Nous avons expliqué au début de la première partie que le pirate informatique appartenait à des réseaux, c'est-à-dire des « *organisations clandestines constituées d'un certain nombre de personnes en relation directe ou indirecte les unes avec les autres.* »[168]

Les réseaux sont des entités connues en criminologie. Hérité des années 80, le paradigme de l'organisation criminelle comme entreprise a été remplacé dans les années 90 par celui du réseau criminel. Aujourd'hui, une bonne partie de la doctrine considère que toute organisation criminelle peut être considérée comme une entreprise dans ses relations avec l'extérieur, et comme un réseau dans son fonctionnement interne.[169] Les chercheurs sont partisans d'une approche double du réseau cybercriminel : ils suggèrent de mêler à l'analyse financière une analyse des réseaux sociaux, aucune des deux n'étant viable de façon autonome sur le long terme.[170]

Dans cette logique, nous montrerons d'abord que les cybercriminels s'organisent en réseaux extrêmement structurés et hiérarchisés, qui ont une tendance à trouver une expression géographique (**Titre I**). Ensuite, nous rappellerons quels facteurs compliquent une approche financière indépendante de toute étude du réseau criminel (**Titre II**).

Titre I : La physionomie des réseaux

Les données personnelles s'échangent sur de véritables marchés noirs en ligne, sur lesquels se côtoient des pirates agissant seuls puis revendant le produit de leurs larcins, et des grands réseaux de *hackers* (**Chapitre 1**). Cette offre variée et volumineuse a donné à cette économie parallèle un profil très particulier, où la demande est reine et la concurrence impitoyable (**Chapitre 2**).

168 Centre National de Ressources Textuelles et Lexicales, dictionnaire en ligne, entrée « Réseau » [en ligne] (consulté le 20 août 2015) http://www.cnrtl.fr/definition/réseau.
169 Gendarmerie royale du Canada, Direction des services de police communautaires, contractuels et autochtones, Sous-direction de la recherche et de l'évaluation, LEMIEUX Vincent, *Les réseaux criminels*, Ottawa, mars 2003, 26 pp..
170 *Des chercheurs créent un algorithme pour analyser les réseaux cybercriminels*, Diplomatie digitale, 21 avril 2015 [en ligne] (consulté le 20 août 2015) http://www.diplomatie-digitale.com/featured/surete/influence-reseaux-cybercriminels-1626.

Chapitre 1 : Des *hackers* organisés en marchés noirs de la donnée personnelle volée

Les marchés noirs en ligne ont fait leur apparition en réponse à l'expertise que requiert la bonne exploitation des données personnelles volées (*section 1*). Initialement un terrain de jeu pour les hackers individuels en quête d'un afflux d'argent, ils sont maintenant envahis par les réseaux criminels qui leur faisaient autrefois concurrence (*section 2*). Ces réseaux sont à présent captés par des organisations criminelles classiques (*section 3*).

Section 1 : L'existence de marchés noirs en ligne comme une réponse à la difficulté de mener de front la captation et l'exploitation de la donnée personnelle

Il existe aujourd'hui des places de marchés *underground* où s'échangent des données personnelles. Elles seraient si nombreuses que les marchés noirs en ligne seraient en concurrence, incitant leurs organisateurs à offrir les meilleures conditions possibles à leurs utilisateurs. Certains proposeraient ainsi des activités *d'escrow*[171] et des garanties : si la carte de crédit a expiré ou été annulée par l'utilisateur, le site rembourse l'acheteur ou remplace la carte inutilisable, etc.

Ces marchés noirs auraient même des centres d'appels, guidant les fraudeurs du web dans l'exploitation des données volées – des cartes de crédit, en particulier. Certaines manœuvres pérennisant la fraude, en changeant les informations de contact correspondant à la carte bancaire, par exemple, nécessitent des compétences en ingénierie sociale. Désormais, certaines places de marché en ligne mettent des spécialistes de cette activité frauduleuse à la disposition des escrocs.

Les frais d'entrée sur ces places sont tels qu'ils compensent largement le coût de l'accueil : jusqu'à plusieurs milliers de dollars pour la seule inscription. Les clients de ces sites s'en disent d'ailleurs généralement satisfaits car la dépense initiale assure du sérieux des vendeurs comme des acheteurs et tient les *rippers* à l'écart. D'autres mesures accompagnent ce prix d'entrée, comme la nécessité d'être parrainé par un ou plusieurs utilisateurs ou l'expulsion rapide des utilisateurs dont le comportement laisserait à désirer. En conséquence, malgré l'anonymat de rigueur sur ces sites, les produits qu'on s'y échange apparaissent généralement d'excellente qualité.[172]

À côté du site de vente lui-même, les cyberdélinquants échangent des astuces et préparent des

171 Voir lexique, entrée **Escrow**.
172 CHRISTIN Nicolas, *Traveling the Silk Road: A measurement analysis of a large anonymous online marketplace*, Université Carnegie Mellon, College of Engineering's cybersecurity laboratory (CyLab), Pittsburgh, Pennsylvanie, États-Unis, 1er août 2012, « *Customer satisfaction* », p. 14.

transactions sur des forums utilisateurs, également hébergés dans le *deep web*.[173]

L'exemple le plus connu est sans doute *Silk Road*, *darknet* [174] anonymisé par le réseau TOR[175] et l'utilisation du *bitcoin*. Il se spécialisait dans le trafic de stupéfiants. Fermé une première fois par le FBI en octobre 2013, ce réseau a ressuscité par la suite. Il a été l'objet de nombreuses études scientifiques, dont il faut relativiser l'apport à ce travail : le règlement intérieur de *Silk Road* interdisait l'échange de données personnelles et de tout ce qui « *aurait pu nuire à quelqu'un.* » Nous n'utiliserons donc les conclusions des scientifiques l'ayant étudié que pour établir un certain nombre de généralités sur les marchés noirs en ligne.

Ils notaient que le gros des transactions concernait de petites quantités et de petites sommes. Il y a plusieurs facteurs qui relativisent ce constat.

D'abord, les vendeurs de qualité reconnue et fournissant de gros volumes réalisaient des ventes privées, qu'il n'était possible de rejoindre que sur invitation. Ainsi, dans le cadre de l'opération qui a permis l'arrestation de Ross William Ulbricht (*Dread Pirate Roberts*), un agent fédéral américain sous couverture a contacté directement l'administration du site et réussi à vendre un kilogramme de drogue via *Silk Road*.

Ensuite, l'accès à ce site particulier était conçu pour être le plus aisé possible et attirer un public très large. Il ne s'agissait pas de mettre en contact des criminels professionnels endurcis, ce qui explique que son focus ait plutôt porté sur de petites transactions. Enfin, la plupart des livraisons, comme pour tout site de vente en ligne, se faisait par la Poste. Les vendeurs dissimulaient de petites quantités de drogue dans leur correspondance, ce qui n'aurait pas été possible pour de plus gros volumes. Les données personnelles volées sont comparativement extrêmement faciles à échanger.

En revanche, un constat tiré de l'étude de *Silk road* semble pouvoir être étendu à tous les marchés noirs en ligne : ils favoriseraient les fournisseurs néophytes et ponctuels. Dans le cadre de *Silk road*, une étude sur huit mois, entre 2011 et 2012, signalait, sur les 600 vendeurs moyens actifs à tout moment sur le site, que seule une soixantaine avaient maintenu une présence continue.[176]

À côté des marchés noirs tels que *Silk road*, dont l'assise morale est floue, vue sa nature de pharmacie en ligne parallèle, des sites se spécialisent dans les échanges dont la nature malfaisante n'est plus à démontrer, comme les données personnelles. A côté des codeurs qui créent les instruments de la cybercriminalité et des usagers moins sophistiqués (*smurfers*, acheteurs ponctuels

173 MARVÃO Susana, *Plongée dans le monde des cybercriminels*, Revue Silicon, 2 décembre 2014 [en ligne] (consulté le 20 août 2014) http://www.silicon.fr/plongee-monde-cybercriminels-103081.html.
174 Voir lexique, entrée **Darknets**.
175 Voir lexique, entrée **TOR**.
176 *Traveling the Silk Road*, op. cit., « *Who is selling ?* », p. 10.

et observateurs), ces marchés noirs hébergent tout le trafic de données personnelles.[177]

Cette vocation les rend instables. Ne bénéficiant pas de la même indulgence qu'une pharmacie en ligne, dans le monde virtuel, ils peuvent être piratés, comme *Carders*, forum allemand dont des pirates ont volé la base de données clients en 2010. La concurrence féroce qu'ils se livrent peut d'ailleurs tourner à la cyberguerre, comme en 2006, lorsqu'un tel site, *CardersMarket*, s'est lancé dans l'acquisition agressive de ses concurrents, piratant leur contenu et leurs clients.[178]

Le *hacking* de *Carders*, comme la facilité d'accès de *Silk road*, a représenté une aubaine pour les scientifiques curieux de ces marchés noirs et qui déplorent leur manque de transparence. L'analyse des données clients du site a mis en lumière l'existence de réseaux structurés en ligne.

Section 2 : La concurrence des réseaux de *hackers*

Les criminologues d'Outre-Atlantique se penchent avec enthousiasme sur l'étude des réseaux criminels, dont les enseignements permettent de lutter contre les activités criminelles avec plus d'efficacité. La criminologie canadienne, en particulier, a appliqué les enseignements de l'étude des réseaux à la forme de criminalité organisée la plus importante sur ce territoire : les activités des gangs de bikers. Il s'agit d'une tendance ancienne, observable dès la fin des années 80.[179]

Ils ont été d'une importance majeure dans la lutte contre le crime organisé, c'est-à-dire la criminalité commise par « *un groupe structuré de trois personnes ou plus existant depuis un certain temps et agissant de concert en vue de commettre une ou plusieurs infractions graves* ».[180] Sous cette étiquette, on retrouve 80 % de l'activité cybercriminelle.

Étudiées sous forme de réseaux, les organisations criminelles apparaissent comme des points (leurs

177 Voir **Annexe 6 : Pyramide des différents participants aux marchés noirs de la cybercriminalité**.
178 ZETTER. Kim, *Vigilantes Hack Criminal Carding Forum and expose underground dealings*, Wired, Security, 19 mai 2010 [en ligne] (consulté le 20 août 2015) http://www.wired.com/2010/05/carderscc/.
179 Voir, par exemple, TREMBLAY Pierre, LAISNE Sylvie, CORDEAU Gilbert, SHEWSHUCK Angela et MCLEAN Brian, *Carrières criminelles collectives : évolution d'une population délinquante (groupes de motards)*, Criminologie, vol. 22, n° 2, 1989, p. 65-94. Cette tendance est toujours d'actualité (lire, pour illustration, ROCHEFORT-MARANDA Catherine, *Analyse de la position des groupes et des individus dans un réseau criminel structuré autour des motards criminalisés*, Mémoire de l'École de Criminologie, Université de Montréal, août 2010, 159 pp. [en ligne] (consulté le 11 septembre 2015) https://papyrus.bib.umontreal.ca/xmlui/bitstream/handle/1866/4908/Rochefort-Maranda_Catherine_CRM_2011_memoire.pdf;jsessionid=546E02EA0C431B73877F76C17AE2E26F?sequence=2).
Un élan académique a été donné en France dès le début des années 2000 pour promouvoir cette section de la criminologie (Voir, par exemple, HAUT François (dir.), *Les gangs de motards criminalisés, Mémoire* de l'Institut de Criminologie de Paris, Département de recherche sur les Menaces Criminelles Contemporaines, Université de Paris II (Panthéon - Assas), août 2001, 160 pp.).
180 *Convention des Nations Unies contre la criminalité organisé*e, signée à New York, le 15 novembre 2000 [Convention de Palerme], en vigueur le 29 septembre 2003, article 2 « Terminologie », alinéa a.

membres) reliés entre eux par des connexions, à la fois directes et indirectes. Ces structures sont toutes différentes, plus ou moins denses (leurs connexions sont plus ou moins redondantes.) Pour les forces de l'ordre, cette densité est synonyme de solidité car elle signifie que la destruction d'un ou plusieurs nœuds (l'arrestation d'un ou plusieurs membres) n'entravera pas le réseau de façon significative.

Par ailleurs, la force ou la faiblesse des connexions est un bon indicateur des facteurs qui incitent des cybercriminels à collaborer. Les chercheurs remarquent des facteurs récurrents : les liens du sang, les liens générationnels, les liens créés par le voisinage, la participation passée aux mêmes associations, les liens ethniques, nationaux ou culturels. La compréhension de ces facteurs de cohésion guide les enquêteurs dans leur analyse et leur approche des organisations.

Un autre élément intéressant est la centralité de chaque acteur, qui le rend plus ou moins intéressant pour les forces de l'ordre. Elle peut être définie de trois façons : la centralité de degré dépend du nombre de liens directs qu'un acteur a avec les autres acteurs du réseau (capital social d'un acteur), la centralité de proximité est la longueur cumulée des plus courts chemins reliant un acteur aux autres acteurs d'un réseau, l'acteur central étant celui dont la longueur cumulée est la plus petite (efficacité de la communication de l'acteur dans le réseau), la centralité d'intermédiarité dépend de la fréquence à laquelle l'individu sert d'intermédiaire entre deux acteurs utilisant le plus court chemin pour communiquer (importance stratégique de sortir l'acteur du réseau). La centralité d'articulation, une variante de l'intermédiarité, réfère d'ailleurs à l'acteur dont la disparition produit la plus grande fragmentation dans le réseau.[181]

Cette notion de réseau apparaissait très secondaire tant que l'on considérait les *hackers* comme travaillant en isolation les uns des autres mais les analyses les plus récentes s'inscrivent en faux contre cette hypothèse.

Suite au piratage de *Carders*, notamment, les scientifiques ont étudié différents réseaux de cyberdélinquants et leur morphologie. L'existence et la pérennité de ceux-ci s'expliqueraient par le besoin d'assurances des cybercriminels. En effet, comme on l'a expliqué, les marchés de données personnelles volées semblent moins fiables que la moyenne des marchés noirs en ligne. En utilisant des programmes similaires à ceux qu'utilisent les réseaux sociaux, les scientifiques s'efforcent de mesurer l'influence de chaque membre de ces réseaux. Comme dans une organisation criminelle classique, celle-ci semble être fonction de l'expérience engrangée par chaque membre et de sa notoriété dans l'organisation : il faut gravir les échelons et prouver sa valeur.

181 *Les réseaux criminels*, op. cit., pp. 7-9.

Il faut distinguer deux modèles de réseaux cybercriminels : les « gangs » et les « cartels ».[182]

Les gangs semblent peu structurés, se regroupant autour d'un décideur fort. L'entrée dans un gang inclut un processus de sélection très rigoureux. Leur force est aussi leur faiblesse : ils tirent parti des opportunités financières qui se présentent. Ils sont donc très flexibles quant à leurs activités mais leur manque d'organisation les limite dans leur développement financier. Alors que les priver de leurs sources de revenus paraît voué à l'échec, l'arrestation de leur leader suffit à les disperser.

Les cartels sont beaucoup plus organisés, davantage spécialisés. Ils ont une véritable stratégie de développement centrée sur la rentabilisation. Ils sont bien plus denses. Au lieu d'une figure centrale, ils s'organisent autour de plusieurs nœuds de taille moyenne, « les cadres supérieurs de l'organisation ». Ces cadres peuvent être responsables de filiales, différentes communautés interconnectées, qui se différencient soit géographiquement, soit par leur spécialité, soit pour d'autres motifs, plus difficiles à discerner. Il semble plus facile de rentrer dans un cartel, donc de l'infiltrer mais il est plus difficile de le paralyser, vue la redondance des connexions internes.[183]

La plupart des chercheurs conseillaient aux forces de l'ordre de s'attaquer à l'élément de confiance pour que les réseaux de *hackers* s'effritent d'eux-mêmes, mais cette tactique trouve ses limites. En effet, ces dernières années, les réseaux cybercriminels ont manifesté une certaine tendance à s'implanter géographiquement, ce qui leur permet de renforcer leurs facteurs de cohésion interne et facilite le démembrement des activités entre les mains de spécialistes.

Section 3 : L'apparition de démembrements non-virtuels des réseaux cybercriminels

Il faut bien remarquer que certains points du globe ont vu apparaître une véritable industrie cybercriminelle. Ainsi, une ville roumaine, perchée dans les Alpes Transylvaniennes, Râmnicu Vâlcea, est surnommée aujourd'hui « Hackerville ».[184] Les Français connaissent également de nombreuses arnaques venues d'Afrique : l'arnaque nigérienne, la captive égyptienne, l'arnaque à l'amour ivoirienne, etc. L'Asie-Pacifique, avec 60 % des piratages de programmes dans le monde,

182 Voir **Annexe 25 : Réseaux criminels : le modèle du gang** et **Annexe 26 : Réseaux criminels : le modèle du cartel**.
183 *Des chercheurs créent un algorithme pour analyser les réseaux cybercriminels*, Diplomatie digitale, 21 avril 2015 [en ligne] (consulté le 20 août 2015) http://www.diplomatie-digitale.com/featured/surete/influence-reseaux-cybercriminels-1626.
184 Documentaires : DUNNE Sean, « The most dangerous town on the Internet », Norton Symantec, 19,59 minutes [en ligne] (consulté le 20 août 2015) http://us.norton.com/mostdangeroustown/index.html#!/en-US et BRAN Mirel, « Roumanie : "Hackerville", capitale de l'arnaque sur Internet », France 24, 17 minutes [en ligne] (consulté le 20 août 2015) http://www.dailymotion.com/video/xvof5p_roumanie-hackerville-capitale-de-l-arnaque-sur-internet_news.

n'est pas en reste.[185] La carte des cybermenaces reproduite en annexe 27 illustre cette dynamique.[186]

Quels facteurs ont fait de ces trois régions de tels centres du cybercrime ?

Un facteur est bien sûr la pénétration sur Internet de ces régions,[187] illustrée en annexe 2.[188] Elle est moyenne ou forte malgré le peu d'utilisation d'Internet par les générations de leurs parents et grands-parents, qui signifie qu'elle est essentiellement imputable aux trentenaires et à leurs cadets. Les moyens mis à leur disposition sont d'ailleurs excellents en Europe de l'Est. Le réseau Internet de la Roumanie, par exemple, est à la pointe de la technologie.

Les primo-entrants sur le marché du travail de ces régions sont aussi confrontés à une économie en crise où l'emploi est rare ou peu attractif. Ce manque de perspectives facilite le recrutement de cyberdélinquants dans des populations jeunes, rompues à Internet et désœuvrées.

Ces pays partagent une histoire politique faite de dictatures qui a donné un caractère militant à Internet : on sait quel rôle la toile a joué dans les Printemps Arabes, de quel pouvoir subversif elle est encore porteuse en Chine. De même, nos voisins d'Europe de l'Est, longtemps privés de la liberté d'expression par des dictatures communistes, défendent l'accès à un Internet libre et anonyme.[189]

Il existe néanmoins de grosses différences entre ces réseaux : certains représentent une expansion des réseaux criminels classiques, certains sont endogènes, d'autres exogènes.

En Russie, le crime organisé classique a vite découvert les avantages que présentait la cybercriminalité, au point de délaisser leurs activités passées à son profit.[190] L'attrait de ces nouvelles activités était d'autant plus évident que les lois russes sont en retard et que les sanctions encourues par les pirates russes ne sont pas réellement dissuasives. Les États dont les ressortissants sont victimes d'attaques par des criminels russes demandent aujourd'hui systématiquement l'extradition. En effet, lorsque des tribunaux russes jugent les *hackers*, ils sont généralement condamnés à des peines avec sursis.

Le niveau d'organisation caractéristique de ces réseaux leur permet de capter d'énormes revenus : en 2011, les criminels russophones se seraient ainsi accaparé plus du tiers du marché mondial de la

185 FLOREAN Alejandro, GANTZ John, KUMAR SRISTI LAKSHMI Sravana, LEE Richard, LIM Victor, MADHAVAN Logesh, NAGAPPAN Mangalam et SIKDAR Biplab, *The Link between Pirated Software and Cybersecurity Breaches How Malware in Pirated Software Is Costing the World Billions*, Université Nationale de Singapour et International Data Corporation (IDC), Étude conjointe IDC #247411, mars 2014, 35 pp..
186 Voir **Annexe 27 : Carte en temps réel des cybermenaces**.
187 Voir lexique, entrée **Pénétration sur Internet**.
188 Voir **Annexe 2 : Carte de la pénétration mondiale sur Internet**.
189 En Roumanie, par exemple, la fondation CEATA défend la liberté digitale sous la forme d'un groupe informel depuis le 10 juin 2008 et en tant que fondation depuis le 15 février 2013. Site de CEATA (consulté le 20 août 2015) https://ceata.org/.
190 Group-IB, *State and trends of the "Russian" digital crime market*, 2011, 32 pp..

cybercriminalité. Il s'ensuit une spécialisation à l'intérieur même du pays, des organisations développant une expertise dans l'envoi de *spams*,[191] d'autres dans la fraude en ligne ou encore dans les attaques *DDoS*.[192] Les échanges entre ces réseaux représentent des sommes considérables (environ 2,3 milliards de dollars en 2010). Les spécialistes qualifient ceux-ci de « marché C2C » (« du crime au crime »).

En Roumanie, les organisations sont plus localisées et moins importantes. Si certaines villes, comme Râmnicu Vâlcea, représentent des points chauds de la cybercriminalité, ces criminels ne cherchent pas encore à étendre le champ de leurs activités à d'autres, plus violentes. Il est encore rare, dans les Carpates roumaines, de recourir aux services d'un garde-du-corps.[193]

L'activité cybercriminelle a adopté une forme si localisée pour des raisons pratiques. La confiance, élément nécessaire du réseau, est plus aisément développée entre des individus qui appartiennent à la même localité et se connaissent depuis des années. Le démembrement du crime en est d'autant plus aisé. Ainsi, à Râmnicu Vâlcea, le gros de la fraude n'est pas le trafic de données personnelles mais plutôt la fraude en ligne – la vente en ligne d'objets qui n'existent pas. Les escrocs roumains se répartissent la tâche, certains d'entre eux se chargeant de la transaction en ligne, d'autres, les flèches, récupérant l'argent et d'autres mettant au point l'« histoire », l'élément de l'arnaque qui doit mettre la cible en confiance, ce qui inclut la traduction dans sa langue et les contacts téléphoniques avec elle.

Les pirates de *Hackerville* recrutent dans le cercle de leurs connaissances, offrant aux débutants de gravir les échelons, faisant leur éducation et leur fournissant du matériel. La proximité géographique assure la formation en même temps qu'une relation de confiance au sein des réseaux. Vu leur caractère endogène, ils bénéficient d'une indulgence de la population, ce qui, considérant l'ascension sociale assurée aux *hackers,* contribue au renouvellement incessant de leurs effectifs.[194]

Le problème du recrutement et du soutien de la population s'est posé en des termes différents aux phénomènes locaux de cybercriminalité exogène. Ainsi, Dakar, comme le reste du Sénégal, voit se développer la criminalité informatique à une vitesse qui laisse les observateurs perplexes.[195] Le phénomène était au départ exogène, le fait de criminels étrangers attirés par la promesse d'un Internet de qualité et peu cher. La pauvreté de la population a permis à ces premiers

191 Voir lexique, entrée **Spam**.
192 Voir lexique, entrée **DDoS**.
193 BHATTACHARJEE Yudhijit, *How a Remote Town in Romania Has Become Cybercrime Central*, Wired, Magazine, 31 janvier 2011 [en ligne] (consulté le 20 août 2015) http://www.wired.com/2011/01/ff_hackerville_romania/.
194 BRAN Mirel, *Les pirates roumains d'"Hackerville" tiennent tête aux polices du monde entier*, Le Monde, 28 décembre 2011 [en ligne] (consulté le 20 août 2015) http://www.lemonde.fr/europe/article/2011/12/28/les-pirates-roumains-d-hackerville-tiennent-tete-aux-polices-du-monde-entier_1623331_3214.html.
195 DIALLO Ismaila, *Un profil des marchés criminels à Dakar*, Rapport 264, Institut d'Études de Sécurité (ISS), août 2014, 12 pp..

cyberdélinquants de s'assurer de sa complicité. Elle leur était en effet indispensable pour rester anonymes et intraçables dans leurs activités criminelles. Le recrutement a été rapide, d'abord comme complices, puis en remplacement des premiers éléments immigrés.

Aujourd'hui, le cybercrime à Dakar est surtout le fait de Sénégalais. De façon intéressante, pourtant, au contraire de nombreux hauts lieux de la délinquance informatique, les risques encourus par les victimes de la cybercriminalité affectent tant leur intégrité physique que leurs données personnelles. Une forme d'arnaque à l'amour particulièrement dangereuse s'est en effet développée dans la grande ville sénégalaise : la cible est appâtée sur un site de rencontre et, non contente d'exiger transfert de fonds après transfert de fonds, sa « dulcinée » finit par l'inviter à venir la rencontrer. Arrivée à Dakar, la victime est séquestrée et les cybercriminels demandent une rançon à sa famille.[196]

Le durcissement des réseaux de cybercriminels sous forme d'organisations criminelles polyvalentes est bien engagé. Le trafic de données ne représente qu'une fraction de leurs activités. Financièrement très attractive, puisqu'elle permet de générer des gains importants au prix d'efforts moindres, elle devrait se développer. L'étude du réseau présente un intérêt particulier pour cibler les individus-clés au sein d'une organisation donnée et lutter efficacement contre le phénomène. Elle ne se suffit pas : comment repérer les organisations elles-mêmes, pour les démanteler ? Vu l'anonymat des marchés noirs en ligne, peut-être l'enquêteur doit-il suivre la seule denrée constante : l'argent. Quel visage présente alors l'économie cybercriminelle à l'enquêteur financier ?

196 Thies Vision, *Séquestration et demande de rançon - La Dic démantèle un réseau de cybercriminels nigérians à Nord-Foire*, 21 août 2015 [en ligne] (consulté le 20 août 2015) http://www.thiesvision.com/Sequestration-et-demande-de-rancon-La-Dic-demantele-un-reseau-de-cybercriminels-nigerians-a-Nord-Foire_a12436.html et *Ils enlèvent, séquestrent puis exigent une demandent de rançon à des Norvégiens : ça se passe à Dakar*, Actusen, Société, 20 juin 2014 [en ligne] (consulté le 20 août 2015) http://www.actusen.com/ils-enlevent-sequestrent-puis-exigent-une-demandent-de-rancon-a-des-norvegiens-ca-se-passe-a-dakar/.

Chapitre 2 : Une économie de la demande favorisant la concurrence

La cybercriminalité constitue une industrie aux énormes profits. Les experts estiment qu'elle coûterait chaque année à l'économie globale entre 375 et 575 milliards de dollars, soit plus que le produit national brut de la plupart des pays.[197] Cette économie très attractive est devenue une économie de la demande face à la multiplication des pirates fournisseurs de données personnelles (*section 1*). Face à cette concurrence, l'offre s'est améliorée et diversifiée (*section 2*). Les prix ont baissé, avantageant les trafiquants générant le plus de données - donc les plus organisés (*section 3*).

Section 1 : La surpopulation en *hackers* individuels

Il est assez naturel que le nombre de pirates informatiques explose avec l'aise grandissante de la pénétration sur Internet. Dans la plupart des pays, la jeunesse est de plus en plus éduquée et connectée. Ces internautes se lancent dans le cybercrime pour des raisons variées. Une récente opération française, menée conjointement avec Europol et appelée « Opération Mousetrap », a consisté en une traque européenne d'acheteurs de logiciels de piratage, les RATs.[198]

Tentés par une criminalité qui leur semblait sans risque, ces pirates étaient pour l'essentiel des jeunes gens, convaincus d'avoir couvert adéquatement leurs traces (en utilisant TOR et les monnaies virtuelles) et de ne courir aucun risque physique.[199] Animés par des motivations diverses, allant de l'objectif purement mercenaire au voyeurisme, ils étaient conscients que les ordinateurs qu'ils infectaient valaient sur les marchés noirs où ils avaient acheté leurs RATs.

Malgré leurs connaissances informatiques quasiment nulles, ils pouvaient extraire les données personnelles, notamment bancaires, les identifiants bancaires (*VBV*) valant entre 12 et 28$ et les cartes de crédit s'échangeant entre 4 et 35$ l'unité ou simplement revendre ces ordinateurs zombies sur des marchés où ils valent jusque plusieurs milliers de dollars.[200]

197 *Net Losses: Estimating the Global Cost of Cybercrime - Economic impact of cybercrime II*, Center for Strategic and International Studies et MacAfee, juin 2014, 24 pp..

198 PONCET Guerric, *Europol a annoncé vendredi matin avoir mené une action coordonnée sur le continent européen. Les suspects sont essentiellement des « débutants »*, Le Point, 21 novembre 2014 [en ligne] (consulté le 20 août 2015) http://www.lepoint.fr/chroniqueurs-du-point/guerric-poncet/operation-mousetrap-lescybergendarmes-s-attaquent-aux-petits-criminels-du-net-21-11-2014-1883176_506.php.

199 Au contraire des cybercriminels africains (*Un profil des marchés criminels à Dakar*, op.. cit.), les Roumains semblent peu enclins à la violence physique (*How a Remote Town in Romania Has Become Cybercrime Central* , op. cit.), de même que les cybercriminels asiatiques (*The Link between Pirated Software and Cybersecurity Breaches*, op. cit.).

200 Voir **Annexe 7 : Valeur des données personnelles *hackées*** et **Annexe 8 : Catalogue des marchés noirs de données personnelles**.

La sophistication technologique que suppose la cybercriminalité tend vers 0. La majorité des systèmes sont vulnérables,[201] la cybersécurité coûte cher et les propriétaires de sites Internet investissent a minima dans ce domaine, même lorsqu'ils ont pleine conscience des dangers qui guettent en ligne.[202] De plus, il est facile d'apprendre les bases du piratage informatique en ligne.[203] Cette éducation n'aurait pas à être très approfondie pour permettre la collecte irrégulière de données personnelles. L'utilisation des instruments du piratage est devenue particulièrement aisée. Ils sont disponibles en ligne à très bas prix : dans le catalogue des prix fourni en annexe 8,[204] un *RAT* revient à moins de 50 dollars, un *exploit kit*[205] se loue entre 600 et 1800$ par mois et un tutoriel[206] coûte entre 1 et 3$. Ce catalogue illustre également une tendance que la plupart des spécialistes confirment : la baisse des prix sous la pression d'une offre devenue endémique.[207]

Il faut noter qu'à l'échelle d'Internet, il s'agit d'une évolution ancienne, remarquée dès le début des années 2010. La baisse des prix enregistrée ne fait que confirmer la transition du cybercrime vers une économie de la demande. Un autre symptôme de ce changement de paradigme tient à l'amélioration de l'offre : les services vendus se sont diversifiés et s'assortissent désormais de petits à-côtés destinés à donner au vendeur un avantage sur la concurrence.

Section 2 : La grande diversité des services procurés

La cybercriminalité comme échange de services est un paradigme aujourd'hui si affirmé que les entreprises spécialisées dans la cybersécurité en sont venues à établir une classification de ces services aux fins de lutte contre le phénomène. Ainsi, MacAfee distingue :

- la recherche comme service : c'est essentiellement la recherche de failles de cybersécurité, ce qui constitue une zone grise du monde informatique, certains *hackers* vont rechercher des vulnérabilités pour les exploiter et d'autres pour les revendre aux grandes sociétés[208] ;

201 Documentaires, op. cit..
202 Le site de *Silk road* a ainsi été catalogué en utilisant un simple robot d'indexation (voir lexique, entrée **Robot d'indexation) :** *Traveling the silk road*, op. cit..
203 Le site hackbbs.org, par exemple, est un terrain d'entraînement à destination des pirates informatiques.
204 Voir **Annexe 8 : Catalogue des marchés noirs de données personnelles** et *Underground Hacker Markets*, DELL Secure Works, décembre 2014, pp. 12-13.
205 Voir lexique, entrée **Exploit kit**.
206 Voir lexique, entrée **Tutoriel**.
207 *Underground Hacker Markets*, op. Cit., p. 1 : « *The Underground Hacker Markets are Booming with Counterfeit Documents, Premiere Credit Cards, Hacker Tutorials and 100% Satisfaction Guarantees.* » (« *Les marchés noirs de pirates informatiques débordent de documents contrefaits, de cartes bleues premium, de tutoriels de hacking et sont 100 % garantis.* »)
208 Voir lexique, entrée **Zero Day**.

- le cybermatériel comme service : il s'agit de créer des logiciels, malveillants ou non (incluant des virus mais aussi des robots d'indexation, par exemple), ou des *exploits* et de les revendre, ainsi que le *hardware* nécessaire à certaines fraudes et certains piratages[209] ;
- l'infrastructure du cybercrime comme service : il ne s'agit plus de concevoir les outils de la criminalité mais de les mettre en œuvre, par exemple en louant un réseau de *bots* pour se livrer à une attaque *DDoS* ou en engageant un service de *spamming* pour diffuser un virus.[210]

Il faudrait y ajouter un type de produits du cybercrime qui se vend de plus en plus : la donnée personnelle raffinée et prête à l'emploi. Alors qu'une *fullz* ne vaut que 30 à 45$, son exploitation sous forme de faux papiers est très rentable (passeports entre 200 et 500$, carte de sécurité sociale entre 250 et 400$, permis de conduire entre 100 et 150$, nouvelle identité complète d'à peu près 250$ avec, pour 100$ supplémentaires, une facture justificative).

Chacun de ces services a été amélioré au cours des dernières années pour attirer des consommateurs toujours plus nombreux et les organisations les fournissant sont de plus en plus interdépendantes.

Quant à la vente des outils de la cybercriminalité, l'apparition de grandes catégories est frappante : l'*exploit kit*, qui permet le piratage d'un site et intéresse surtout les pirates en quête d'informations précises, le *doxxing*,[211] fréquent dans le monde des sociétés et compagnies, le réseau d'ordinateurs zombies, qui sert tant aux spammeurs qu'aux amateurs de l'attaque *DDoS*, l'attaque *DDoS* elle-même, particulièrement du goût des *hacktivistes*, les *ransomwares*,[212] les fameux *RATs* et le *hardware*, qui se décline autour de la fraude à la carte bleue, principalement.

Il faut signaler que, dans chacun de ces domaines, les vendeurs manifestent un sens du marketing bien développé. Ainsi, les programmeurs s'efforcent de développer le logiciel le plus accessible et agréable à utiliser : c'était un des grands points forts du *RAT BlackShades*. Ils se dotent de slogans (« *BlackShades, an easy and powerful way to remote control* »).[213] Ils proposent aussi, à l'image des grandes entreprises, des mises à jour régulières, voire des contrats de licence d'utilisateur final, comme le concepteur du *RAT* ZeuS, en 2008, face aux tentatives de rétro-ingénierie.[214][215]

Les marchés noirs et leurs services après-vente interviennent au niveau de l'infrastructure du crime.

La pression de la demande pour cette amélioration constante, ainsi que la baisse des prix,

209 Voir lexique, entrées **Hardware** et **Skimmer**.
210 PAGET François et SAMANI Raj, *Cybercrime Exposed – Cybercrime-as-a-Service*, McAfee Labs, 2013, 18 pp..
211 Voir lexique, entrée **Doxxing**.
212 Voir lexique, entrée **Ransomware**.
213 *Le logiciel espion Blackshades au cœur d'une grande enquête internationale*, op. cit..
214 Voir lexique, entrées **Contrat de licence d'utilisateur final** et **Rétro-ingénierie**.
215 DUNE Lawrence, *The Hunt for the Financial Industry's Most-Wanted Hacker*, Bloomberg Business, 18 juin 2015 [en ligne] (consulté le 10 août 2015) http://www.bloomberg.com/news/features/2015-06-18/the-hunt-for-the-financial-industry-s-most-wanted-hacker.

favorisent les *hackers* soutenus par une infrastructure qui leur permet de continuer à dégager des profits rendant leur entreprise rentable et de satisfaire les exigences du consommateur.

Section 3 : Les avantages d'un marché à la baisse pour le *hacker* organisationnel

Face à la baisse des prix, les pirates informatiques doivent générer des volumes toujours croissants de données personnelles pour maintenir leurs revenus ou augmenter le potentiel d'exploitation de chaque donnée personnelle qu'ils captent.

Le pirate individuel cherche à exploiter au maximum les données personnelles auxquelles il a accès – tendance que le crime organisé semble épouser en Afrique, où des fraudes sophistiquées et très étendues sur la durée, comme les arnaques à l'amour, se multiplient. Plutôt que la revente, le *hacker* individuel se lance plutôt dans les opérations de chantage à la webcam, dans la *sextorsi*on, ou le rançonnement en ligne.[216] Une variante très populaire du rançonnement en ligne consiste à bloquer l'ordinateur de la victime en se réclamant des forces de l'ordre et à l'accuser d'une infraction quelconque, pouvant aller de la consultation de contenus pédopornographique à la violation du droit d'auteur et d'exiger le paiement d'une « amende » en échange du déblocage de la machine.

Dans les deux cas, l'arnaque a un caractère épisodique et joue sur les sentiments de culpabilité ou de honte de la victime. Ces cybercriminels s'apparentent aux maîtres-chanteurs de notre univers non-virtuel. La sensibilisation des populations semble être la seule vraie solution.[217]

Le marché parallèle de données personnelles paraît au contraire concentré entre les mains du cybercrime organisé. Cette prédominance est renforcée par les mécanismes d'entrée sur les marchés noirs. Avant de débourser plusieurs milliers d'euros pour rejoindre un forum d'échanges de données (ou d'infrastructures et de matériels pour leur acquisition et leur exploitation frauduleuses), le pirate doit être certain que ses gains seront à la mesure de son investissement.

Comme *Silkroad* l'illustrait à merveille, les opportunités les plus intéressantes se cantonnent à des sections de ces *darknets* réservées aux vendeurs sérieux, c'est-à-dire anciens et prolifiques.

Il faut également noter que les marchés de la cybercriminalité souffrent de l'inflation et de la déflation comme les autres, sous l'influence de plusieurs facteurs. Il y a des causes internes à chaque *darknet* : un afflux de données personnelles a ainsi affecté durablement leur prix. Il y a des causes

216 Voir lexique, entrée **Sextorsion**.
217 C'est un des deux propos de l'opération « *Turn Back Crime* », lancée par Interpol, avec l'identification des auteurs de sextorsions : Interpol, *INTERPOL-coordinated operation strikes back at 'sextortion' networks*, 2 mai 2014 [en ligne] (consulté le 10 août 2015) http://www.interpol.int/News-and-media/News/2014/N2014-075.

IRL,[218] dues à l'évolution du coût de la vie dans les régions d'origine des cybercriminels et au comportement de leurs monnaies non-virtuelles. Il y a des causes liées aux monnaies virtuelles elles-mêmes. Ces devises, achetées en ligne à des fournisseurs et intermédiaires, reviendront plus ou moins cher suivant le nombre de commissions, etc. Le cours de la monnaie virtuelle variera suivant les aléas qu'elle connaît sur Internet. Ainsi, l'étude sur *Silk road* que nous citions plus haut a enregistré la brutale perte de valeur du *bitcoin* suite au braquage d'une des principales places d'échange en ligne, Mt.Gox.[219] Ces fluctuations signifient que le seul moyen, pour le cybercriminel, de stabiliser ses revenus est de les inscrire sur le long terme.

Mener des activités sur ces marchés suppose des capacités internes de blanchiment d'argent. Le temps où les pirates de *hackerville* fournissaient simplement leur numéro de compte en banque aux victimes qu'ils trouvaient sur les grands sites d'achat en ligne est en effet depuis longtemps révolu.[220] Les organisations criminelles classiques en disposaient bien sûr avant l'avènement d'Internet. En ce qui concerne les autres, le blanchiment peut se faire par des biais virtuels ou non.

Ainsi, les pirates de Râmnicu Vâlcea optent encore pour l'envoi de flèches. Celles-ci, Roumains émigrés dans des pays occidentaux ou jeunes envoyés en tournées de collecte des profits de la cybercriminalité, se chargent de réceptionner l'argent des victimes dans leur pays, dans des bureaux de transferts de fonds puis de les expédier dans leur ville d'origine (laquelle compte pas moins d'une demi-douzaine de bureaux de *Western Union*). Il s'ensuit que l'activité cybercriminelle suit des cycles. Les Américains, cibles favorites des Roumains, sont devenus familiers des saisons du cybercrime, et se méfient surtout aux alentours de Noël, qui est tous les ans l'occasion d'un pic.[221]

Les moyens de blanchiment virtuel du crime sont donc quasiment indétectables et présentent un défi bien plus affirmé pour l'enquêteur financier.

218 Voir lexique, entrée **IRL**.
219 *Traveling the silkroad*, « *Potential intervention strategies - Attacking the financial infrastructure* », p. 20.
220 *How a Remote Town in Romania Has Become Cybercrime Central* , op. cit..
221 BOTEZATU Bogdan, *Five security scenarios to avoid this Christmas*, ABC, Technology and Games, 19 décembre 2014 [en ligne] (consulté le 20 août 2015) http://www.abc.net.au/technology/articles/2014/12/19/4152115.htm.

Titre II : Une économie parallèle difficile à mesurer

Pour mener une investigation financière efficace, il faut identifier les principaux traits distinctifs de la criminalité concernée en tant que phénomène économique. La cybercriminalité crée toute une économie semi-souterraine. En règle générale, les échanges sont réalisés dans des monnaies virtuelles et sur des places d'échange échappant à toute supervision (**Chapitre 1**). Il s'agit d'un marché en expansion continuelle, sous la pression du *spamming*, qui en constitue la colonne vertébrale (**Chapitre 2**). Cette économie parallèle est aussi vaste et complexe que notre économie *IRL*, elle est pourvue de ses places d'échanges, de ses hauts-lieux du blanchiment d'argent (**Chapitre 3**).

Chapitre 1 : L'anonymat sur les marchés noirs de données personnelles en ligne

Les flux financiers du marché noir des données personnelles sont structurés par l'exigence de rendre intraçable l'argent qu'il dégage. Comme l'illustrent les schémas en annexes 28 et 29,[222] cette qualité est assurée à plusieurs niveaux. D'abord, plusieurs précautions techniques assurent que la surveillance des places d'échange ne puisse remettre en cause l'anonymat des cybercriminels qui les fréquentent (*section 1*). Ensuite, face à une demande croissante et sous la pression des forces de l'ordre, les monnaies virtuelles sont régulièrement perfectionnées dans le sens d'une intraçabilité renforcée (*section 2*). Enfin, attardons-nous sur l'action du *smurfer*, cet intermédiaire incontournable qui assure le blanchiment des fonds (*section 3*).[223]

Section 1 : Les processus d'anonymisation des sites Internet et de leurs utilisateurs

En général, les marchés noirs ne sont accessibles que par le biais du réseau TOR, garantie d'anonymat pour les internautes. Il s'agit d'un groupe de serveurs entretenus par des volontaires qui permet aux utilisateurs de se connecter à Internet par le biais d'autres terminaux, de façon à se rendre intraçables. Normalement, chaque ordinateur se connecte le plus directement possible aux serveurs Internet qu'il vise. TOR, au contraire, conçoit des chemins d'accès qui brouillent les

222 Voir **Annexe 28 : Le circuit financier de la cybercriminalité** et **Annexe 29 : L'anonymisation des flux financiers de la cybercriminalité**.
223 Voir lexique, entrée **Money remittance**.

pistes.[224]

Les criminels ne sont pas les seuls à utiliser TOR : il attire les dissidents politiques de la plupart des dictatures à travers le monde, des journalistes mais aussi des particuliers soucieux de discrétion, particulièrement pour leurs activités intimes en ligne (groupes de soutien en ligne, etc). S'attaquer à TOR, c'est remettre en question la possibilité de rester anonyme sur Internet. Or, la doctrine s'entend sur le fait que l'anonymat sur Internet est une composante essentielle du droit dans un pays démocratique.[225]

Le réseau a été bâti tout entier autour de ce concept et de celui de respect de la vie privée, ce qui fait obstacle à toute forme d'autocensure. Les terminaux servant de relais, pavant le chemin d'accès sont appelées « nœuds » (*nodes*). Le dernier d'entre eux, nommé « nœud de sortie » (*exit node*), prend un risque tout particulier, puisqu'il peut être théoriquement tenu pour responsable de toute activité qu'il relaie dans la plupart des législations nationales. Il lui est théoriquement loisible de surveiller et modifier les données qui transitent par son biais.[226] Le site du projet l'interdit strictement, tout en reconnaissant que des difficultés juridiques peuvent résulter de ce blanc-seing. Le résultat a été une certaine baisse des vocations au rôle de nœud de sortie.[227]

Il est également techniquement très difficile d'abattre TOR et la quasi-unanimité des communautés d'experts informatiques, de *hackers* et de la doctrine scientifique assure une base participative considérable pour l'amélioration du service. L'hébergement des sites de marché noir se fait en revanche suivant des procédés beaucoup plus sensibles éthiquement.

Ces sites sont hébergés sur des hébergeurs *bulletproof*, c'est-à-dire plus ou moins complaisants.[228] Ils cumulent plusieurs torts aux yeux des autres acteurs d'Internet : ils participent au *spamming*, hébergent des contenus illicites (*malware*,[229] *phishing*, etc) et détournent les techniques à disposition des hébergeurs.[230] En conséquence, ils font l'objet de sanctions internes aux FAI et aux FSI. Les premiers leur infligent surtout le désappairage, c'est-à-dire leur refusent l'appairage et évitent de contribuer à leur trafic Internet. Parmi les FSI, les moteurs de recherche surtout vont pouvoir pratiquer le déréférencement systématique des pages.[231]

224 Voir schémas en **Annexe 30 : Schémas de fonctionnement de TOR**.
225 CHAWKI Mohamed, *Anonymity in Cyberspace: Finding the Balance between Privacy and Security*, Droit-Tic, juillet 2006, 24 pp..
226 SENET Régis, *À TOR et à travers – Anonymat et utilisation malveillante*, XMCO, Revue ActuSecu, Numéro 39, janvier 2015, pp. 7-16.
227 The TOR Project, Questions-Réponses, « Problèmes légaux » [en ligne] (consulté le 20 août 2015) https://www.torproject.org/eff/tor-legal-faq.html.
228 Voir lexique, entrées **Hébergeur bulletproof** et **Hébergeur Internet**.
229 Voir lexique, entrée **Malware**.
230 Voir lexique, entrée **Black SEO**.
231 Voir lexique, entrées **Appairage**, **Déréférencement** et **Moteur de recherche**.

L'ICANN a aussi pu sanctionner les hébergeurs *bulletproof*.[232][233] Le site Internet *Spamhaus* tient plusieurs listes de serveurs *bulletproof* suivant les contenus et sites qu'ils hébergent. Il est surtout destiné à assister les différentes boîtes mails pour qu'elles distinguent les *spams* du reste du courrier électronique. Les listes des dix pays, des dix hébergeurs *bulletproof* et des dix opérations émettant le plus de *spams* sont reproduites en annexes 31, 32 et 33. Elles illustrent bien l'existence de paradis pour ces hébergeurs.[234] Parmi les dix plus accueillants de ceux-ci, figurent au moins deux États membres de l'Union européenne : le Royaume-Uni, sixième, et l'Allemagne, huitième. Néanmoins, avec 382 et 342 opérations de *spamming* répertoriées respectivement, ils sont loin derrière les trois premiers États de la liste : les États-Unis (2743), la Chine (1341) et la Russie (962).

Il faut dire que les responsabilités des hébergeurs varient grandement d'un État à l'autre. Dans l'Union européenne, leur principale responsabilité est la conservation des données. La directive 2006/24/CE sur la conservation des données de l'Union européenne, du 15 mars 2006, comprend un article 6 exigeant la conservation des données pendant une période allant de six mois à deux ans. Ces données incluent pour Internet celles permettant de retrouver et d'identifier la source et la destination d'une communication, d'en déterminer la date, l'heure et la durée, en déterminer le type, identifier le matériel de communication des utilisateurs, le localiser.

L'imprécision du délai a posé des difficultés, en laissant une grande marge aux législateurs nationaux. En France, c'est le décret n°2006-358 du 24 mars 2006 relatif à la conservation des données des communications électroniques qui fixe cette durée de conservation à un an. Doivent être conservées les informations permettant d'identifier l'utilisateur, excluant strictement la conservation du contenu des correspondances. La CJUE a récemment invalidé la directive.[235]

Au contraire de l'utilisation de TOR ou du problème des hébergeurs *bulletproof*, boudés par le législateur européen, les monnaies dématérialisées, devises de rigueur sur les marchés noirs de données personnelles, ont fait l'objet d'une prise en compte assez précoce. Dès le 18 septembre 2000, la directive 2000/46/CE a vu le jour. Son imprécision et son impopularité ont conduit à sa révision par la directive 2009/110/CE du 16 septembre 2009. Celle-ci semble ne pas suffire puisque, encore le 27 janvier 2015, lors de la réunion des Ministres des Finances des 28 États membres, certains, dont le représentant français, ont demandé de nouvelles mesures en réponse aux implications des devises virtuelles en matière de blanchiment d'argent.[236]

232 Voir lexique, entrée **ICANN**.
233 ICANN, *Suppression du registraire EstDomains*, 11 décembre 2008 [en ligne] (consulté le 20 août 2015) https://www.icann.org/news/announcement-2008-11-12-en.
234 Voir **Annexe 31 : Dix plus actifs pays émetteurs de *spams***, **Annexe 32 : Dix plus actifs hébergeurs *bulletproofs* émetteurs de *spams*** et **Annexe 33 : Dix plus actives opérations de *spamming***.
235 CJUE, Affaires jointes C-293/12 et C-594/12, 8 avril 2014, *Digital Rights Ireland et Seitlinger e.a.*.
236 DUCOURTIEUX Cécile, *Les Européens se fixent des règles pour lutter contre le blanchiment*, Le Monde, 27

Section 2 : La sophistication des monnaies virtuelles

Pour mieux comprendre l'impopularité de la directive 2000/46/CE, il faut distinguer les monnaies dématérialisées les unes des autres. Cette directive porte sur la monnaie électronique, la définit comme une valeur monétaire représentant une créance sur l'émetteur, stockée sur un support électronique, émise contre la remise de fonds d'un montant dont la valeur n'est pas inférieure à la valeur monétaire émise et acceptée comme moyen de paiement par des entreprises autres que l'émetteur. Elle est bien dématérialisée mais elle conserve un lien avec les monnaies traditionnelles car les fonds sont exprimés dans la même unité de compte. C'est l'exemple des porte-monnaie électroniques, à ne pas confondre avec les services de paiement sans contact (qui ne relèvent que d'un procédé technique car les unités de compte sont matériellement stockées sur la carte bancaire).

La monnaie virtuelle n'a plus ce lien avec les monnaies classiques, elle est dotée de sa propre unité de compte qui n'a pas de statut légal, n'est pas régulée par une banque centrale ni délivrée par des établissements financiers. C'est d'ailleurs le problème des banques centrales, qui estiment que cette indépendance les rend volatiles et les apparente plus à des produits spéculatifs qu'à des monnaies.[237] C'est l'unité de compte stockée sur un support électronique créée par une personne physique ou morale et destinée à comptabiliser les échanges. Ce n'est pas une créance sur l'émetteur, elle n'est pas émise contre la remise de fonds, elle se distingue donc de la monnaie électronique.[238]

Dans ses études, la Banque centrale européenne (BCE) distingue trois catégories de monnaies virtuelles.[239] D'abord, la monnaie virtuelle fermée (type 1 dans le schéma), ne peut être dépensée que dans une communauté virtuelle cloisonnée et ne peut être convertie en monnaie légale. Elle n'entretient aucun lien avec l'économie réelle. Ce sont par exemple les monnaies en usage dans les jeux vidéo. Ensuite, la monnaie virtuelle à flux unidirectionnel (type 2) peut être achetée contre une devise légale à un taux de change défini. En revanche, elle ne peut être reconvertie en monnaie légale. Elle permet néanmoins d'acheter des biens et services dans le monde réel, pas seulement virtuel. Typiquement, les points de fidélité échangeables contre des produits relèvent de cette catégorie. Enfin, la monnaie virtuelle à flux bidirectionnel (type 3) peut être convertie dans une

janvier 2015 [en ligne] (consulté le 20 août 2015) http://www.lemonde.fr/europe/article/2015/01/27/les-europeens-se-fixent-des-regles-pour-lutter-contre-le-blanchiment_4564622_3214.html.

237 Banque Centrale Européenne, *Virtual currency schemes – a further analysis*, février 2015, p. 23.

238 RAULT Raphaël, *Monnaie virtuelle et monnaie électronique : distinction et encadrement contractuel des porte-monnaie virtuels affectés*, LexisNexis, Tendance Droit, 28 juin 2015 [en ligne] (consulté le 20 août 2015) http://www.tendancedroit.fr/monnaie-virtuelle-et-monnaie-electronique-distinction-et-encadrement-contractuel-des-porte-monnaie-virtuels-affectes/.

239 Voir **Annexe 35 : Les trois types de monnaies virtuelles selon la BCE**.

monnaie légale, d'où l'existence d'un cours d'achat de monnaie et d'un cours de revente. Au sein de celles-ci, ajoutons une distinction entre monnaies virtuelles à flux bidirectionnel et à émetteur centralisé et monnaies virtuelles à flux bidirectionnel et à émetteurs multiples en réseau.

La traçabilité de ce troisième type de monnaies est problématique. Elle se présentera différemment suivant que la monnaie privée dématérialisée sera émise par une société, autorité centrale, ou par un réseau d'émetteurs décentralisés. Ce dernier cas regroupe le *Bitcoin* et les monnaies virtuelles qu'il a inspirées, les *altcoins*,[240] au nombre desquelles : *Litecoin*, *Pandacoin*, *Applecoin*, etc.[241]

Au contraire de *Perfect Money*, *Liberty Reserve, Web Money* et leurs consœurs, les *bitcoins* sont générés par minage. La monnaie, créée en 2009, est par nature cryptographique.[242] Chaque *bitcoin* est caractérisé par sa chaîne de blocs, dont chacun retrace une transaction passée, authentifiée par un mineur, suivant le processus schématisé en annexe 36.[243] L'activité de mineur est rentabilisée par le minage, c'est-à-dire la création de *bitcoins*. La monnaie a été conçue pour que cet afflux en nouvelles espèces ralentisse avec le temps. Le minage est généralement réalisé par des sociétés ou des individus spécialisés, qui sont en bon nombre et ne constituent pas des émetteurs centralisés

Les intermédiaires principaux dans la vie du *Bitcoin* sont les sociétés spécialisées dans leur change en monnaie réelle.[244]

Ce fonctionnement limite théoriquement l'anonymat des échanges en *bitcoins* mais il n'existe pas, à notre connaissance, d'instruments de surveillance des flux de *bitcoins* exploitant les chaînes de blocs sur une grande échelle. Cet anonymat partiel est appelé « pseudo-anonymat ». La plupart des crypto-monnaies partagent ce trait. L'existence de briques d'anonymat adaptables aux *bitcoins*[245] et d'*altcoins* anonymes comme *Darkcoin*,[246] laisse à penser que la pression du marché et l'intense compétition entre programmeurs pourraient doter *Bitcoin* d'un anonymat absolu.[247]

À la différence de *Bitcoin*, les monnaies virtuelles à flux bidirectionnel et à émetteur

240 Voir lexique, entrée **Altcoins**.
241 GUINIER Daniel, *Monnaies virtuelles Le cas Bitcoin pourquoi tant d'emballement?*, Revue du GRASCO, n°12, avril 2015, pp. 37-52.
242 Voir lexique, entrée **Crypto-monnaie**.
243 Voir **Annexe 36 : Projection du nombre total de *bitcoins* telle que présentée par la BCE**.
244 Note du Centre de Recherche de l'École des Officiers de la Gendarmerie Nationale (CREOGN), France, *Monnaies virtuelles : nature et risques*, septembre 2014, Note numéro 6, 4 pp. et **Annexe 37 : Fonctionnement de *Bitcoin***.
245 GREENBERG Andy, *'Zerocoin' Add-on For Bitcoin Could Make It Truly Anonymous And Untraceable*, Forbes, 12 avril 2013 [en ligne] (consulté le 20 août 2015) http://www.forbes.com/sites/andygreenberg/2013/04/12/zerocoin-add-on-for-bitcoin-could-make-it-truly-anonymous-and-untraceable/.
246 Site français de Bitcoin, *Les altcoins anonymes*, 6 juillet 2014, Explications [en ligne] (consulté le 20 août 2015) http://france-bitcoin.net/2014/07/les-altcoins-anonymes/.
247 KOPSTEIN Joshua, *Gold 2.0: can code and competition build a better Bitcoin ? Zerocoin and Ripple present two ways to improve the ailing crypto-currency*, The Verge, 23 avril 2013 [en ligne] (consulté le 20 août 2015) http://www.theverge.com/2013/4/23/4252808/can-zerocoin-and-ripple-build-a-better-bitcoin.

centralisé dépendent, pour leur émission, d'une autorité d'émission centralisée, généralement une société constituée dans un paradis fiscal.[248] Dans le cas de la défunte monnaie virtuelle *Liberty Reserve*, il s'agissait d'une société du même nom dont les actes constitutifs avaient été déposés au Costa Rica. Elle émettait la monnaie, gérait les porte-monnaie électroniques la contenant et les transactions réalisées entre eux.

Elle vendait sa monnaie exclusivement à une poignée de grossistes privés aussi installés dans des pays dont la législation restait laxiste. Ceux-ci la revendaient à un groupe d'échangeurs privés qui la mettaient à disposition des particuliers. Il fallait, pour obtenir des *LR*, créer un compte. La manœuvre était rapide et simple, sans aucune vérification d'identité. Il ne fallait à l'utilisateur que fournir une adresse mail comme point de contact, les noms et prénoms donnés n'étant l'objet d'aucune vérification. Après validation du compte, l'utilisateur obtenait un numéro de compte qui lui permettait d'effectuer des transactions avec d'autres internautes.

Liberty Reserve enregistrait les adresses IP des terminaux accédant au compte. Pour utiliser la monnaie virtuelle en tout anonymat, il aurait suffi d'utiliser TOR, de fournir un nom et un prénom fictifs et d'ouvrir une adresse mail dans ce but exprès.[249] Cette dépendance à un émetteur central s'est avérée être le principal talon d'Achille de ce dernier type de monnaies virtuelles.

Le 28 mai 2013, la société et une demi-douzaine de ses membres fondateurs et administrateurs ont été mis en accusation par le Procureur de New York pour conspiration de blanchiment d'argent, transfert de fonds d'origine criminelle et conspiration et exercice de la profession d'intermédiaire financier sans licence. L'enquête et les arrestations ont impliqué les forces de l'ordre de 17 pays.[250]

L'impact le plus ressenti de l'affaire a été le gel des 45 comptes bancaires de la société. L'argent des utilisateurs est passé entre les mains des autorités américaines. Néanmoins, celles-ci ont mis en place un système de remboursement des fonds dont la provenance peut être justifiée. Seuls les cybercriminels ont souffert de ce coup dur et ils ont appliqué par la suite une stratégie de répartition de leurs fonds entre les différentes monnaies virtuelles qui leur donne des assurances contre la mise hors-jeu des différentes autorités émettrices de monnaies virtuelles.[251] Le point fort de ce type de monnaies virtuelles n'est pas la perfection de chacune mais leur simple prolifération.

248 Voir **Annexe 38 : Fonctionnement de la monnaie virtuelle *Liberty Reserve***.
249 CEIS, op. cit., pp. 44-51.
250 KALLENBORN Gilbert, *Monnaies virtuelles : un réseau de blanchiment mondial a été mis à jour*, 01net, 29 mai 2013 [en ligne] (consulté le 20 août 2015) http://www.01net.com/editorial/596389/monnaie-virtuelles-un-reseau-de-blanchiment-mondial-a-ete-mis-a-jour/#?xtor=EPR-1-[NL-01net-Actus]-20130529.
251 EVEN Maxence, GREY Aude et LOUIS-SIDNEY Barbara, Étude *Monnaies virtuelles et cybercriminalité Etat des lieux et perspectives*, Compagnie Européenne d'Intelligence Stratégique (CEIS), Collection Notes Stratégiques, Technologies de l'information, 10 avril 2014, « Non, Perfect Money ne remplace pas Liberty Reserve », pp. 9-13.

Ces monnaies bénéficient aussi des différences entre les législations des États membres de l'UE. Les directives de l'Union européenne visent davantage les monnaies électroniques et les établissements de monnaie électronique. Les États membres sont libres de leur législation en matière de monnaies virtuelles. Le simple volume des échanges pourrait inciter les législateurs à leur proposer un encadrement : la législation fiscale notamment a dû s'accommoder du *Bitcoin*. Doit-il être traité en bien ou en marchandise comme en Chine ou en Corée du Sud, en revenus du capital, comme aux États-Unis ou en « monnaie privée » comme en Allemagne ?[252]

Plusieurs pays imposent les transactions en monnaies virtuelles, sans établir pour autant un statut juridique clairement défini, ce qui pose des difficultés en matière de lutte contre le blanchiment d'argent. En Chine ou au Japon, les échanges de *bitcoins* ne sont permis qu'entre particuliers. En Russie, il leur est attaché, comme à toute monnaie virtuelle, une présomption de participation à des opérations illégales. En France et aux États-Unis, les plate-formes doivent s'enregistrer auprès du *Financial Crimes Enforcement Network* (*FinCEN*) chargé de la lutte anti-blanchiment.[253] Cet encadrement ne suffit pas et, en juin 2014, en France, le groupe de travail « Monnaies virtuelles » a suggéré un correctif en trois volets, incluant l'encadrement de leur utilisation (plafonnement de l'utilisation des monnaies virtuelles comme méthodes de paiement, contrôle des flux et limitation de l'anonymat des utilisateurs de monnaies virtuelles), la régulation et la coopération (adaptation du dispositif de lutte contre le blanchiment d'argent et le financement du terrorisme aux risques posés par les monnaies virtuelles et les activités les utilisant et harmonisation de la régulation au niveau européen et international).[254]

L'anonymat est préservé par l'utilisation de monnaies virtuelles mais, à l'entrée dans l'économie réelle, ce sont les intermédiaires de blanchiment des gains cybercriminels qui l'assurent.

Section 3 : Le recours à un intermédiaire faisant écran à la surveillance des gains cybercriminels

En anglais, le verbe « *to smurf* » désigne la mise en œuvre d'une architecture des

252 NESTLER (von) Franz, *Deutschland erkennt Bitcoins als privates Geld an*, Frantfurter Allgemeine Ginanzen, 16 août 2013 [en ligne] (consulté le 20 août 2015) http://www.faz.net/aktuell/finanzen/devisen-rohstoffe/digitale-waehrung-deutschland-erkennt-bitcoins-als-privates-geld-an-12535059.html.
253 HERRY Valentine et PÉCASTAING Juliette, *Les Bitcoins, nouvelle monnaie virtuelle : quels enjeux?*, Revue Sorbonne OFIS, octobre 2014, 4 pp..
254 *L'encadrement des monnaies virtuelles – Recommandations visant à prévenir leurs usages à des fins frauduleuses ou de blanchiment*, Groupe de travail « Monnaies virtuelles », TRACFIN, Ministère des Finances et des Comptes publics, juin 2014, 10 pp..

transactions financières consistant à les diviser en plusieurs petites opérations pour éviter l'attention des autorités. Par extension, le « *smurfer* » est l'individu dont l'activité fait écran entre les enquêteurs et le criminel, soit lors de la fourniture de matériel à ce dernier, soit dans l'utilisation de ses gains illicites. Dans le contexte de la cybercriminalité, c'est la personne qui transfère de la part d'un tiers, par le biais d'un service postal ou d'un service électronique, des fonds acquis illégalement.[255]

Ces *smurfers* peuvent être victimes eux-mêmes, comme la *money mule*, ou volontaires, comme les flèches.[256] Ils protègent l'identité et la localisation du criminel[257] et offrent des assurances : l'appartenance culturelle, ethnique ou l'expatriation de la flèche, l'ignorance de la *money mule*, l'absence de risques juridiques pour le *drop*.[258]

Le *smurfer* intervient dans l'avant-dernière phase de circulation des flux financier de la cybercriminalité, « la phase de monétarisation », juste avant le blanchiment d'argent. Il utilise principalement des instruments de transfert financier qui ne devraient pas être anonymes mais qui le deviennent, comme *Ukash*, *Western Union*, ou d'autres systèmes de transfert instantané de fonds.

Ukash peut être achetée en magasins dans 55 pays différents à travers le monde. Aucune pièce d'identité n'est nécessaire pour échanger de l'argent liquide contre un bon et, surtout, contre le code de 19 chiffres noté dessus. Il peut servir à acheter des biens sur de nombreux sites dans l'anonymat le plus total. Ce mode de paiement très prisé par les criminels est en croissance constante (de l'ordre de 65 % par an).[259] Il représenterait pour plus de 700 millions d'euros de transactions annuelles.[260]

Money Gram et *Western Union* fonctionnent de façon assez similaire. Elles permettent l'envoi instantané d'argent liquide à travers le monde. En théorie, les transferts sont nominaux. Un individu se rend dans un point de vente et indique les nom, prénom et nationalité du bénéficiaire. Il remet ensuite à l'agence un montant en liquide, que le bénéficiaire retirera également en liquide dans une autre agence. Il existe des restrictions à l'envoi et à la réception, liées à leur caractère nominatif. Leur montant maximum est d'environ 7 600 euros par jour et par personne, en France, par exemple.

255 DELEPIÈRE Jean-Claude, *21ème Rapport d'activités*, Cellule de traitement des informations financières (CTIF), Belgique, Bruxelles, 2014, « Cas 3 – Utilisation de tierces personnes », pp. 72-73.
256 Voir lexique, entrée **Smurfer**.
257 DESANTIS Matthew, DOUGHERTY Chad, MCDOWELL Mindi, *Understanding and Protecting Yourself Against Money Mule Schemes*, United States Computer Emergency Readiness Team (US-CERT), 22 juin 2012, https://www.us-cert.gov/security-publications/understanding-and-protecting-yourself-against-money-mule-schemes.
258 Documentaires, « The most dangerous town on the Internet » et « Roumanie : "Hackerville", capitale de l'arnaque sur Internet », op. cit..
259 Voir **Annexe 39 : Fonctionnement de Ukash** et **Annexe 40 : Conseils aux vendeurs Ukash pour la remise des bons**.
260 HART Matthew, PAGET François, SAMANI Raj, *Le blanchiment numérique Analyse des monnaies virtuelles et de leur utilisation à des fins criminelles*, Livre blanc, McAfee Labs, 2013, 17 pp..

Dès lors que la condition d'identification a été contournée, ces restrictions ne valent plus. Or, elle est rarement respectée. *Western Union* est prête à agréer tout commerçant disposant d'un ordinateur et d'une connexion Internet. Elle lui offre uniquement une formation à la lutte contre le blanchiment d'argent et une assistance en la matière. En échange, tous les commerçants agréés sont responsables de leurs activités dans le domaine. La société américaine l'explique clairement sur son site Internet.[261]

Money Gram a un meilleur réseau de distribution encore : la société est présente dans plus de 200 pays et territoires. Les transferts en agence ne requièrent que de l'argent liquide et la pièce d'identité de l'expéditeur. Il aura besoin d'une référence de transfert à 8 chiffres et de ses papiers d'identité, avec les mêmes problèmes pour faire respecter cette politique.[262]

Il faut signaler le désintérêt croissant des cybercriminels pour la plate-forme de paiement en ligne *PayPal*. Celle-ci se conforme aux directives de l'UE depuis plusieurs années, demandant des justificatifs aux titulaires de comptes comptant 2500€ ou plus. Ce changement de politique – et le gel desdits comptes – a d'ailleurs soulevé de nombreuses protestations parmi les utilisateurs du service. [263] Peut-être cette docilité s'explique-t-elle par le caractère centralisé de *PayPal*. La société, qui a déposé des statuts sur quatre continents, opère en son nom propre dans chacun de ceux-ci. Constituée en 1993 au Luxembourg, *PayPal* (Europe) est supervisée par la Commission de Surveillance du Secteur Financier et soumise à la réglementation luxembourgeoise, y compris celle issue du droit de l'Union européenne.[264] Fondée en 1998 à Palo Alto, Californie, sa filiale américaine fait de même. Son antenne indienne reçoit aussi des instructions de la banque nationale. En Australie, elle est même assimilée à une banque et doit respecter les mêmes régulations.

Le respect de ces politiques de lutte contre la corruption est garanti par l'identification de ses clients, lesquels doivent enregistrer leur compte en banque ou leur carte bancaire pour utiliser le service.

Quant à la phase de monétarisation, une meilleure répartition des responsabilités entre agents agréés et systèmes de transfert international de fonds ainsi qu'une obligation de justification pour les comptes participant au déplacement de grosses sommes semblent indispensables. Les montants dégagés par l'économie parallèle cybercriminelle devraient se détacher du volume des transactions internationales en liquide. Les réseaux d'échange de données personnelles génèrent des sommes importantes. La cybercriminalité, en règle générale, est un pan de l'économie en croissance

261 Voir **Annexe 41 : Politique de *Western Union* sur le blanchiment d'argent**.
262 MoneyGram, Transfert d'Argent MoneyGram [en ligne] (consulté le 20 août 2015) http://www.moneygram.fr/le-service-moneygram.
263 Voir **Annexe 42 : Le 23 février 2013, un usager de *PayPal* proteste sur le forum d'aide de la société, suite au gel de son compte** et **Annexe 43 : Les trois étapes de l'inscription sur *PayPal***.
264 Ce qui inclue les textes de la réforme anti-blanchiment d'argent sur laquelle on reviendra.

constante, sous la pression des « véhicules » du cybercrime que sont les *spams*.

Chapitre 2 : Le *spamming*, maillon faible de l'économie du cybercrime

Les *spams*, qui représentent l'immense majorité des communications échangées tous les jours,[265] constituent l'échine de l'économie parallèle du cybercrime. Ils garantissent un afflux massif et régulier de fonds, assurant au minimum l'entretien des infrastructures de la cybercriminalité (*section 1*). Ils interviennent également à tous les niveaux, de la captation des données personnelles à leur rachat et leur utilisation frauduleuse (*section 2*) mais tout en restant vulnérables aux investigations, ainsi qu'aux attaques des pirates et des opérateurs informatiques (*section 3*).

Section 1 : Le *spamming*, un raz-de-marée économique

Le *spam* est un courrier électronique qui se caractérise par un envoi massif et souvent répété à des personnes avec lesquelles l'expéditeur n'a jamais eu de contact et dont il a récupéré les adresses électroniques de façon irrégulière. C'est aussi un phénomène à la progression aussi constante qu'alarmante. En 2001, on estimait qu'il représentait environ 10 % de tout le courrier électronique échangé. En 2004, ce chiffre avait atteint les 50 %.[266] En 2006, il atteignait les 80 %.[267] Depuis 2009, il avoisine les 90 %.[268]

Le *spamming* représente un coût considérable pour les entreprises, principalement à cause du temps que perdent leurs employés à trier communications légitimes et *spams*. La perte de revenus engendrée pour chaque entreprise représenterait l'équivalent du salaire annuel d'un employé sur dix.[269]

Les États membres ont tous légiféré, optant pour l'une de deux approches : « *opt-in* » et « *opt-out* ». Dans la première option, l'envoi de messages ne peut se faire sans le consentement préalable des destinataires. Dans le second cas, l'envoi de messages à toutes les personnes qui ne s'y opposent pas est autorisé. L'Union européenne, pour sa part, a choisi l'« *opt-in* » par la directive n° 2002/58/

265 Voir **Annexe 44 : Projection du pourcentage des courriers électroniques qualifiables de *spams***.
266 Commission Européenne, *Communication COM(2004) 28 final sur les communications commerciales non sollicitées ou "spam"*, 22 janvier 2004 [en ligne] (consulté le 20 août 2015) http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=celex:52004DC0028.
267 Ministère de la Culture et de la Communication, *Le « spam »*, 4 avril 2007, 13 parties [en ligne] (consulté le 20 août 2015) http://www.culturecommunication.gouv.fr/Politiques-ministerielles/Industries-culturelles/Dossiers-thematiques/Le-spam.
268 EGEDIAN, « Solutions antispam pour les entreprises » [en ligne] (consulté le 20 août 2015) http://www.egedian.com/antispam/spam-en-entreprise.
269 Vade-Retro, « Combien vous coûte le spam ? » [en ligne] (consulté le 20 août 2015) http://www.vade-retro.com/fr/cout_spam.asp.

du 12 juillet 2002 relative à la vie privée et aux communications électroniques, que les États membres devaient transposer avant le 30 octobre 2003.

Le Royaume-Uni fait figure d'exception. Alors qu'un système d'*opt-in* est de rigueur avant tout envoi de *spam* à un particulier, les entreprises ont seulement le droit à l'*opt-out* lorsque le « pourriel » est adressé à des adresses électroniques professionnelles contenant des données personnelles.

Certains États, comme l'Italie, ont en revanche transposé le système d'*opt-in* et l'ont adjoint d'une définition très large du *spam*, complètement indépendante du support de communication et du contenu du message.[270] Ces dispositions s'accompagnent d'un code de déontologie des pratiques sur Internet et de lois sur le commerce électronique mais la violation de ces dispositions n'est punie que par des amendes et des réparations civiles. Il en va de même en Lituanie.[271] Les deux États membres participent par ailleurs à l'accord de coopération du réseau de contact des autorités anti-spam (CNSA), leurs autorités de lutte contre le *spam* partagent des informations et s'efforcent d'instruire des plaintes dépassant les frontières, tout comme celles de l'Autriche, la Belgique, Chypre, la République tchèque, le Danemark, la France, la Grèce, l'Irlande, Malte, les Pays-Bas et l'Espagne.[272]

A l'inverse, certains États laissent des agents privés mener la majeure partie de la lutte contre le *spamming*. Par exemple, alors qu'en France et dans la plupart des membres de l'Union européenne, c'est une autorité publique indépendante qui tient la boîte à *spams*, en Allemagne, l'association des fournisseurs de services Internet, l'*Eco Verband*, s'en charge.[273]

Juridiquement comme économiquement, le *spamming* est un phénomène remarquable et les spammeurs sont des opérateurs à part. Malgré leur particulière adaptabilité, ils représentent en effet un poids économique considérable. Il se situe dans une aire grise de l'économie, à mi-chemin entre cybercriminalité et e-marketing. Les spammeurs se considèrent d'ailleurs, dans leur immense majorité, comme de simples businessmen. C'est particulièrement vrai pour les Russes, qui ciblent surtout les Américains. Dans ce cadre, le *spam* est apparu comme un simple outil de promotion des pharmacies de contrebande en ligne. Il s'agissait surtout, au début, de fournir aux citoyens des États-

270 Le *Code pour la protection des données personnelles* en vigueur le 1er janvier 2004 précise la définition du spam.
271 Lituanie, *Loi sur la protection du consommateur*, articles 19, *Loi sur la publicité*, 31 juillet 2000, article 9, *Loi sur les télécommunications*, 5 juillet 2002, *Loi sur la protection légale des données personnelles*, 1er janvier 2001, *Ordonnance du Ministère de l'économie sur l'approbation de la vente et des contrats de fourniture négociés au moyen des télécommunications*, 24 août 2004, *Loi sur l'approbation des régulations sur la fourniture de services particuliers de la société de l'Information* et *Loi sur les communications électroniques*, 15 avril 2004, transposant la directive 2002/58/CE.
272 Commission Européenne, IP/05/146, Bruxelles, 7 février 2005, *Les pays européens s'allient pour combattre le "spamming" (envoi non sollicité de courriels)* [en ligne] (consulté le 20 août 2015) http://europa.eu.int/information_society/topics/ecomm/highlights/current_spotlights/spam/index_en.htm.
273 Site de l'association (consulté le 20 août 2015) https://www.eco.de.

Unis des produits pharmaceutiques qui leur seraient revenus trop cher dans le commerce normal.[274]

On sera alors face à du simple marketing électronique, une forme de *spamming* relativement inoffensif. Le *spamming* se définit en effet moins par son contenu ou son impact que par ses moyens. D'abord, il faut noter qu'aux yeux des opérateurs Internet, en plus de l'usage abusif des messageries électroniques, il inclut la *black SEO* mais aussi la diffusion de messages publicitaires par d'autres biais. En plus du *spam* classique, Internet véhicule des *spams* sur les forums, les blogs, dans les commentaires de différents sites, des *spim* et des *SPIT*.

Cette flexibilité des spammeurs leur permet de tirer parti de leurs relations avec le reste des cybercriminels pour échapper à la détection et au blocage, essentiellement en utilisant des *botnets* dans le cadre du *snowshoe spamming*[275] mais en tirant profit de ces connexions pour compléter leurs revenus en participant à des opérations de *phishing* ou à la conservation et la diffusion de *malwares*.

Section 2 : La place incontournable du *spam* dans les réseaux de cybercriminels

L'intérêt des spammeurs, outre leur visibilité, est cette centralité dans les réseaux de cybercriminels qui trafiquent des données personnelles. Ils interviennent à tous les niveaux du circuit décrit ci-dessus, de la captation de données personnelles au blanchiment des revenus.

Les spammeurs financent par ailleurs une bonne partie des moyens de base de la cybercriminalité. Ils sont les principaux utilisateurs des hébergeurs *bulletproof*, lesquels vont servir nombre de propos pour les *hackers*, hébergeant les sites de marchés noirs de données personnelles, des pages servant au *phishing* ou redirigeant vers de telles pages, tous les moyens de la *black SEO*. Ils permettent également la conservation, l'échange et la diffusion de *malwares*.[276] Parmi ces *malwares*, on en trouve un certain nombre dont la fonction est de créer plus de machines zombies. Les *botmasters* vont aussi pouvoir contrôler leurs *bots* par le biais de ces hébergeurs.

Comme l'indique le schéma en annexe 45, l'envoi de *spams*, pour atteindre de tels volumes, requiert l'utilisation de *botnets*, ces réseaux d'ordinateurs zombies. Les *botnets*, comme les hébergeurs *bulletproof*, sont des outils modulables du cybercrime. Ils peuvent servir plusieurs propos. Ainsi, comme l'illustre l'annexe 46, leur utilisation pour l'expédition de *spams* ne cesse de diminuer. Ils se sont dans leur grande majorité convertis à l'attaque *DDoS* sur commande.[277]

274 KREBS Brian, *Spam nation : the inside story of organized cybercrime—from global epidemic to your front door*, Sourcebooks, Inc, Naperville, Illinois, États-Unis, 18 novembre 2014, 256 pages.
275 Voir lexique, entrée **Snowshoe spamming**.
276 Voir **Annexe 34 : Tableau des types d'opérations répertoriées sur les 10 pires hébergeurs *bulletproofs***.
277 Voir **Annexe 45 : Envoi d'un spam publicitaire** et **Annexe 46 : L'évolution du propos des *botnets* avec le**

Le *spam* lui-même participe à la captation de données personnelles. Plutôt que des messages publicitaires, les spammeurs peuvent participer à des opérations de *phishing* à grande échelle, regroupés sous l'étiquette « fraudes » dans l'annexe 47.[278] Le *spamming* permet également la propagation de *malwares*, soit massive et irraisonnée, soit par une frappe chirurgicale. Le ciblage d'adresses mails professionnelles va permettre d'introduire un logiciel espion[279] dans les systèmes informatiques d'une société et de piller ses banques de données. C'est une des méthodes principales de captation des données personnelles. La collecte d'adresses électroniques dans ce type d'attaque est relativement facile : il existe souvent des annuaires internes à la société relativement publics et, sinon, une attaque annuaire[280] complète efficacement le recueil des quelques adresses mails d'accès facile. Il n'en va pas de même dans les cas d'envoi massif de mails. Dans certains pays qui ont opté pour l'*opt-out*, comme le Canada, dans les premières années de sa législation informatique, le pillage de cette liste rouge s'est révélé très lucratif. Il n'en va pas de même dans les États membres de l'UE. Les spammeurs sont donc devenus de gros acheteurs de données personnelles volées.

Ils participent aussi à la monétarisation, que les trafiquants de données réalisent par le biais de *smurfers*. Dans le cas particulier de la *money* mule, appâtée par une offre d'emploi d'apparence licite, le *spam* participe à son recrutement : constitue une opération de *spamming* le fait de poster de fausses annonces sur des sites de recherche d'emploi, de les adresser à un certain nombre d'adresses mails ou de diriger les internautes vers ces annonces par le biais de la *black SEO*.

Les spammeurs font donc partie intégrante des réseaux de captation et de trafic de données personnelles sur Internet. Or, ils sont sujets aux investigations et à la neutralisation.

Section 3 : La vulnérabilité des spammeurs face aux investigations et à l'interception

Le cas des spammeurs russes est sans doute le mieux documenté. En Russie, le *spamming* n'est qu'un *business* comme un autre. Comme expliqué plus haut, les spammeurs considèrent qu'ils réagissent à une demande économique des populations auxquelles ils s'adressent.

Il y a un autre motif à leur relatif manque de subtilité. Les *adverts*, comme ils aiment à se faire appeler, font figure d'aînés parmi les communautés de cybercriminels. Cette différence de générations est en partie due à la nature d'aire grise du *spamming*, laquelle semble attirer des

temps.
278 Voir **Annexe 47 : Contenus des *spams* (en pourcentage)**.
279 Voir lexique, entrée **Logiciel espion**.
280 Voir lexique, entrée **Dictionnaire**.

délinquants plus matures. De telles opérations nécessitent aussi des infrastructures considérables. Les spammeurs forment des groupes très structurés, que les Russes appellent « *partnerka* » (littéralement « partenariats »). Or, comme le souligne le consultant en sécurité Brian Krebs dans son livre consacré au *spamming*, le commerce parallèle de données personnelles n'est pas né clandestin, il s'est retiré progressivement dans l'ombre, à mesure que les autorités s'y intéressaient.

Les « *sponsors* », des affaires en mal de publicité, engagent des sociétés de marketing. Celles-ci ont d'ores et déjà formé des contrats avec des hébergeurs, les deux appartenant généralement aux mêmes individus, derrière l'écran d'une ou plusieurs sociétés factices. Elles se chargent ensuite de recruter des *botmasters* sur les grands forums de cybercriminels (généralement organisés par grands groupes de langage : anglais, russe, arabe, mandarin, parmi les plus communs). Les *hackers* qui dirigent les *botnets* travaillent généralement de conserve avec des pirates qui se chargent de recueillir les coordonnées nécessaires à l'expédition de leurs larges volumes de *spams*.

Ces délinquants doivent donc garder un ancrage dans les grands forums cybercriminels qui ont fait leur éducation, tout en développant une activité et des relations économiques apparemment légitimes. Cette nature binaire les rend particulièrement repérables, d'autant qu'ils forment un petit monde très cloisonné. *Spam Nation*, de Brian Krebs, qui décrit justement la cybercriminalité russe, s'ouvre sur le récit du décès d'un acteur majeur de ce monde souterrain, Nikolai « Kolya » McColo. Il décrit ses répercussions dans ces termes : « *This was a major event in the cybercrime underworld. Days later, the motley crew of Moscow-based spammers would gather to pay their last respects at his service. The ceremony was held at the same church where Kolya had been baptized less than twenty-three years earlier.* »[281]

Ces spammeurs sont d'autant moins discrets qu'ils imitent les schémas du crime organisé classique, entre chantages, rackets et exécutions sanglantes. L'ouvrage de Krebs retrace d'ailleurs ce qu'il appelle « la guerre pharmaceutique », un affrontement long et coûteux entre deux géants russes du *spam* qui n'ont pas hésité à manipuler les forces de l'ordre sur trois continents pour se débarrasser l'un de l'autre. Non sans ironie, ce sont précisément les armes employées dans ce bras de fer qui ont fini par abattre leurs empire du cybercrime.[282]

Outre leurs guerres intestines, les spammeurs doivent faire face à de nombreux ennemis,

281 *Spam Nation*, op. cit., « Chapitre 1 : Parasite », « Ce fut un événement majeur du monde souterrain de la cybercriminalité. Quelques jours plus tard, la foule hétéroclite des spammeurs moscovites allait se réunir et faire ses adieux lors de l'enterrement. La cérémonie se tint dans la même église où Kolya avait été baptisé, moins de 23 années auparavant. »

282 KREBS Brian, *Russian internet payment boss sentenced*, The Age, 7 août 2013 [en ligne] (consulté le 20 août 2015) http://www.theage.com.au/it-pro/security-it/russian-internet-payment-boss-sentenced-20130805-hv179.

dont les moindres ne sont pas ceux qu'ils surnomment « les *antis* »[283], experts informatiques, FSI, entreprises de sécurité et gérants de listes noires en ligne, tous opposés au *spam*.

En fait, dans la meilleure tradition du crime organisé russe, les spammeurs ont décidé d'engager un bras de fer avec tous ces opposants. Après que le marché du *spam* s'est effondré, dans les années 2000, de nombreux *botmasters* se sont trouvés désœuvrés et très irrités. Une autre activité qui sollicite le concours de *botnets* est la menée d'attaques *DDoS*.[284] Ils ont immédiatement pris pour cible une série de firmes de cybersécurité[285] et de listes noires en ligne,[286] causant un chaos d'épiques proportions sur Internet.[287][288] Les spammeurs n'ont pas pu maintenir ce feu nourri d'attaques : un effort de longue durée requiert de gros moyens humains et ces opérations ne jouissent pas de la même popularité que d'autres amateurs d'attaques *DDoS*, comme les *Anonymous*.[289]

Les autres *hackers* ne souhaitent pas être amalgamés avec eux. Les spammeurs introduisent aussi leurs puissants réseaux de machines zombies pour mener des attaques *DDoS* contre les monnaies virtuelles ou les places de change.[290] Les services mails doivent monopoliser d'importantes ressources électroniques pour éviter que ces envois massifs de courriers électroniques perturbent le reste des internautes et ils représentent un immense manque à gagner pour les entreprises, au point que des sociétés se dévouent intégralement à leur éradication, en plus des antivirus classiques. Leur abus des techniques de la *black SEO* a aussi ostracisé les fournisseurs de service Internet, dont surtout les moteurs de recherche.

Ce front uni de la société civile facilite le travail des forces de police et des journalistes, notamment parce que des acteurs privés n'hésitent pas à dérober des informations aux spammeurs.[291] Ce sont des fenêtres ouvertes sur les réseaux cybercriminels.

283 Voir lexique, entrée **Antis**.
284 FREYSSINET Eric, *Botnets : Illustration de nouvelles formes de criminalité organisée*, Revue du GRASCO, n°6, juillet 2013, pp. 10-18.
285 LEYDEN John, *Blue Security calls it quits after attack by renegade spammer - Folds spam fighting operation*, The Register, 17 mai 2006 [en ligne] (consulté le 20 août 2015) http://www.theregister.co.uk/2006/05/17/blue_security_folds/.
286 JENKINS Quentin, *Second arrest in response to DDoS attack on Spamhaus*, Spamhaus, 7 juillet 2014 [en ligne] (consulté le 20 août 2015) http://www.spamhaus.org/news/article/715/second-arrest-in-response-to-ddos-attack-on-spamhaus.
287 ARÈNE Véronique, *Spamhaus victime d'une gigantesque attaque DDoS*, Le Monde Informatique, 28 mars 2013 [en ligne] (consulté le 20 août 2015) http://www.lemondeinformatique.fr/actualites/lire-spamhaus-victime-d-une-gigantesque-attaque-ddos-53029.html.
288 LAURENT Alexandre, *DDOS sans précédent contre Spamhaus : Internet va bien, merci pour lui*, CLUBIC, jeudi 28 mars 2013 [en ligne] (consulté le 20 août 2015) http://pro.clubic.com/it-business/securite-et-donnees/actualite-550362-spamhaus-ddos-cyberbunker.html.
289 Ces *hacktivistes* utilisent aussi des réseaux d'ordinateurs zombies pour perpétrer leurs attaques par déni de service mais, en général, ces *botnets* sont constitués de volontaires souhaitant participer à une cause : CARIO Erwan, *L'attaque en déni de service, arme d'obstruction massive*, Libération Écrans, 10 décembre 2010 [en ligne] (consulté le 20 août 2015) http://ecrans.liberation.fr/ecrans/2010/12/10/l-attaque-en-deni-de-service-arme-d-obstruction-massive_953288.
290 Dont, par exemple, le braquage de Mt. Gox dont nous avons parlé plus haut.
291 C'est une telle fuite qui a permis à Brian Krebs de mener une étude aussi approfondie des spammeurs russes.

Ces brèves considérations sur le *spamming* illustrent d'abord les mécanismes du marché noir de données personnelles. La confiance n'est pas de rigueur dans ce milieu et la saper semble le moyen le plus efficace de mettre les trafiquants hors-jeu. Pour l'instant, ce sont les guerres intestines des spammeurs qui ont entraîné l'intervention des forces de l'ordre, et non l'inverse, mais cette situation peut se retourner. Ensuite, Internet se situe largement hors du champ d'expertise des forces de l'ordre : elles ne détiennent pas l'essentiel des informations, c'est seulement par le biais des opérateurs privés qu'elles peuvent y accéder. Vus les contacts extensifs des spammeurs, ils pourraient devenir la première étape d'une enquête de taille à paralyser des réseaux cybercriminels très larges, incluant ceux qui trafiquent les données personnelles. Plutôt que de mettre hors d'état de nuire cette catégorie de délinquants informatiques, il pourrait être intéressant de reconstituer toute la filière, avec l'assistance de partenaires privés.

Une autre démarche, que la justice russe emploie fréquemment dans le cas des spammeurs, consiste à se concentrer sur les incriminations de blanchiment d'argent et diverses infractions fiscales.[292] Alors que cette approche paraît plutôt efficace dans le cas de cyberdélinquants proches du crime organisé traditionnel, ceux qui utilisent des instruments novateurs échappent généralement aux enquêteurs financiers.

292 Une méthode à laquelle nos confrères américains se réfèrent toujours comme à « un Capone », du nom de Al Capone, cette légende de la mafia d'Outre-Atlantique, que les services fédéraux, faute de pouvoir prouver ses activités de criminalité organisée, avaient finalement poursuivi pour évasion fiscale.

Chapitre 3 : Une économie parallèle perméable à l'économie numérique

Tous les lieux d'échange en ligne pourraient devenir de hauts lieux du blanchiment d'argent. Plus encore que les casinos « terrestres », les casinos en ligne, en dignes héritiers d'une longue tradition, et les jeux de rôle en ligne permettent le blanchiment d'argent (*section 1*) mais, avec les données personnelles volées, c'est le cas de toute activité économique en ligne (*section 2*).

Section 1 : La facilitation du blanchiment d'argent par les jeux en ligne

Le jeu en ligne favorise le blanchiment des gains illicites issus du trafic de données. Ces sites étaient déjà depuis longtemps un terrain de jeu pour les fraudeurs et les *carders*, les premiers dégageant des revenus par le non-paiement des gains ou la manipulation des taux de redistribution, les seconds pratiquant le vol des cartes bancaires et exploitant celles qu'ils contrôlent déjà.[293] Ils ont vite compris que ces plate-formes offraient des avantages en termes d'anonymat.[294]

Les casinos, qui ont vocation à s'adresser au public le plus large possible, ne s'arrêtent pas aux frontières des États qui les prohibent. Ils assurent donc à leurs utilisateurs qu'ils ne pourront pas être identifiés : l'inscription ne requiert qu'un minimum d'informations personnelles, les monnaies virtuelles, comme les cartes prépayées et la plupart des moyens de paiement, sont prises en charge, ils peuvent fonctionner sur TOR ou à l'abri derrière des serveurs proxy.[295] Ils offrent en général des services de change, entre monnaies fiduciaires et virtuelles et des services de retrait et de dépôt sur comptes faisant intervenir de nombreux intermédiaires.

Leur nombre assure qu'il soit impossible de paralyser le blanchiment d'argent en retirant un ou plusieurs sites, ou un ou plusieurs serveurs, de la circulation. Pour mener une action efficace, les forces de l'ordre n'ont d'autre choix que de faire intervenir leurs collègues d'autres États mais aussi les opérateurs privés, comme les FAI, FSI, les spécialistes de la cybercriminalité ou les banques.

Les spécialistes saluent le travail de l'EC3 (*European Cybercrime Centre*), l'entité spécialisée d'Europol, qui mène une action multiple, de fusion de toute l'information et de toute l'expertise

293 Laboratoire d'EXpertise en Sécurité Informatique, *Cybercriminalité des Jeux en Ligne*, Livre Blanc du CERT-LEXSI, juillet 2006, 21 pp..
294 BARRERE Patrick, *Jeux en ligne. Les mafias entrent en jeu sur les paris sportifs*e, Le Progrès, 11 juin 2013 [en ligne] (consulté le 20 août 2015) http://www.leprogres.fr/economie/2013/06/11/les-mafias-entrent-en-jeu-sur-les-paris-sportifs.
295 Voir lexique, entrée **Proxy**.

technique des polices européennes, et opérationnelle[296], l'EUCTF (European Union Cybercrime Taskforce) et l'ECTEG (European Cybercrime Training and Education Group), d'évaluation des menaces, d'élaboration d'initiatives de lutte contre la cybercriminalité, de formation et de recherche.

Certains ont dénoncé le manque de régulation, notamment fiscale, comme une cause d'utilisation des jeux en ligne pour le blanchiment car il rendrait ces flux d'argent particulièrement difficiles à retracer.[297] Dans les années 2010, des législations ont fleuri à travers toute l'Union européenne.[298] Elles sont largement conformes au cadre général européen fixé en octobre 2012 par la Commission européenne dans son plan d'action pour le secteur des jeux d'argent en ligne, « Vers un cadre européen global pour les jeux de hasard en ligne » et son livre vert.[299]

L'ouverture du secteur des jeux en ligne en 2010[300] a fait de la France un véritable terrain d'expérimentation. En 2006, dans un rapport au Sénat,[301] un expert était cité et indiquait que 90 % de l'activité était à l'époque clandestine. Quand la régulation est aussi stricte que celle qui est de rigueur en France et qu'un Français sur cinq joue en ligne,[302] il est difficile d'imaginer que l'ensemble des sites soit passé dans la légalité. Néanmoins, le consensus sur l'encadrement des sites de paris et de jeu en ligne dans l'UE est tel qu'il les rend très peu attractifs pour la fraude et le blanchiment d'argent.[303]

Une variante du jeu en ligne qui échappe encore largement aux législations européennes est le jeu de rôle en ligne rassemblant beaucoup de joueurs[304] mais le blanchiment en ligne sur ces sites s'apparente davantage au blanchiment sur des sites de e-commerce ou de *trading* en ligne. Il passe en effet par la vente à perte de biens virtuels, la création de gains fictifs ou il se cache derrière une

296 Mise à disposition des États membres de l'expertise technique, analytique et d'investigation numérique nécessaire pour mener des enquêtes en matière de cybercriminalité), d'entretien des partenariats policiers, tant régionaux que mondiaux (avec Interpol, Eurojust (unité de coopération judiciaire de l'Union européenne.

297 Parlement Européen, Commissions: Commission spéciale sur la criminalité organisée, la corruption et le blanchiment de capitaux, 12 novembre 2012, Communiqué de presse n°20121112IPR55400, *Taxer les jeux d'argent en ligne pour lutter contre les activités de la mafia*, 2 pp..

298 Assemblée nationale, Commission des finances, de l'économie générale et du contrôle budgétaire, FILIPPETTI Aurélie et LAMOUR Jean-François, *Mise en application de la loi n° 2010-476 du 12 mai 2010 relative à l'ouverture à la concurrence et à la régulation du secteur des jeux d'argent et de hasard en ligne*, Rapport d'information n°3463, 25 mai 2011 [en ligne] (consulté le 20 août 2015) http://www.assemblee-nationale.fr/13/rap-info/i3463.asp.

299 Autorité de régulation des jeux en ligne (ARJEL), *Rapport d'activité 2013*, 2014, 49 pp. [en ligne] (consulté le 20 août 2015) http://www.arjel.fr/IMG/pdf/rapport-interactif-2013.pdf.

300 France, *Loi n° 2010-476 relative à l'ouverture à la concurrence et à la régulation du secteur des jeux d'argent et de hasard en ligne*, 12 mai 2010 (JO n° 110 du 13 mai 2010).

301 Sénat Français, Commission des Finances, du contrôle budgétaire et des comptes économiques de la Nation, TRUCY François, *L'évolution des jeux de hasard et d'argent*, Rapport d'information n°58, 7 novembre 2006.

302 Observatoire des jeux, France, COSTES Jean-Michel, EROUKMANOFF Vincent, RICHARD Jean-Baptiste, TOVAR Marie-Line, *Notes sur les jeux d'argent en France en 2014*, Les notes de l'Observatoire des jeux, n° 6, avril 2015, 9 pp..

303 European Gaming and Betting Association (EGBA), Factsheet *Anti blanchiment d'argent*, 23 juillet 2010 [en ligne] (consulté le 20 août 2015) http://www.egba.eu/pdf/EGBA_FS_MoneyLaundering_french.pdf.

304 Voir lexique, entrée **MMORPG**.

forme de spéculation sur les places d'échange de ces MMORPG.

Section 2 : L'épanouissement du commerce et de la finance en ligne hors d'un cadre réglementaire suffisant pour empêcher le blanchiment d'argent

Le e-commerce constitue un moyen de blanchiment très pratique pour les cyberdélinquants. En effet, il offre l'avantage de ne contraindre ni le vendeur ni l'acheteur à s'identifier.

Ainsi, les Roumains de *Hackerville*, par exemple, utilisent beaucoup les sites de vente en ligne pour blanchir leur argent. Un des schémas les plus simples consiste à acheter avec leurs devises virtuelles et leurs comptes *off-shore* des biens de grand prix à l'étranger, le plus souvent des voitures, à les importer en Roumanie et, là, à les revendre à perte à des compatriotes. Le prix de revente déclaré est supérieur au prix d'achat. Cette différence permet de dégager un profit factice, qui correspondra en fait aux sommes gagnées sur les marchés noirs de données bancaires.

Évidemment, cette forme de blanchiment suppose le soutien d'un réseau, d'acheteurs nombreux prêts à participer à la machination.

Comme le e-commerce, le *trading* en ligne prend aujourd'hui de l'essor. Il est devenu possible d'investir sur les marchés financiers depuis son ordinateur personnel, voire depuis son téléphone. L'implantation des intermédiaires professionnels dans les paradis fiscaux facilite un abus de cette activité, le blanchiment d'argent via le *trading* en ligne.

Le but originel de cette implantation était d'échapper aux impositions fiscales pour augmenter les profits mais elle a induit une certaine opacité. Une technique parmi de nombreuses autres consistera à créer deux sociétés fictives, à acquérir un certain nombre d'actions de l'une tant qu'elle reste quantité inconnue et que son cours est bas, puis à faire gonfler artificiellement le prix de l'action en investissant massivement depuis l'autre société et à revendre les actions immédiatement. Le cours plongera mais le bénéfice obtenu par la revente est complètement blanchi.

La plupart des autorités européennes s'efforcent de réguler cette activité pour éviter le blanchiment mais la difficulté tient à ce que les *brokers*[305] ne sont généralement pas établis sur leur territoire.[306]

Une utilisation efficace des données personnelles captées irrégulièrement autorise à brouiller

305 Voir lexique, entrée **Courtier en bourse**.
306 Centre d'analyse des opérations et déclarations financières du Canada (CANAFE), *Tendances et typologies en matière de blanchiment d'argent dans le secteur canadien des valeurs mobilières*, Rapports de typologies et tendances, avril 2013, « Risques supplémentaires - le courtage en ligne », pp. 19-20 [en ligne] (consulté le 20 août 2015) http://www.fintrac.gc.ca/publications/typologies/2013-04-fra.pdf.

encore davantage les cartes. Elle permet aussi de multiplier les fausses transactions et d'attribuer les opérations frauduleuses aux victimes dont les données personnelles ont été volées.

Comme on l'a vu, les trafiquants de données personnelles en ligne forment des réseaux hiérarchisés et structurés qui interagissent sur les marchés noirs de la cybercriminalité. La nature d'économie de la demande de ce trafic favorise la généralisation de ce système. Il y a des facteurs qui compliquent une investigation financière de ces réseaux : il y a sur Internet des pans d'économie semi-souterrains (monnaies virtuelles, places d'échange non-régulées, etc) et les pirates recourent à divers moyens pour s'assurer de leur anonymat de l'intraçabilité de leurs échanges (précautions techniques des marchés, monnaies virtuelles, *smurfer*).

Ce marché est en expansion continuelle et il est extrêmement versatile, toutes les activités que les pirates hébergent sont interconnectées, sans pour autant être toutes clandestines. Il a ses places d'échanges et ses hauts-lieux du blanchiment d'argent.

Partie III : Les apports possibles de l'UE à la lutte contre le trafic de données personnelles en ligne

Comme nous l'avons vu, un atout majeur des trafiquants de données personnelles tient au caractère transnational d'Internet. Une coopération internationale est donc indispensable pour mener des actions efficaces contre ces trafics, de même qu'un renouvellement des moyens de lutte. En quoi l'Union européenne peut-elle contribuer à entraver la captation, l'échange et l'usage frauduleux de données personnelles ?

Bien que l'Union européenne ne puisse assumer à elle seule la lutte contre la cybercriminalité et l'usage illicite de données personnelles, elle peut offrir une importante contribution. En effet, il entre dans ses attributions et capacités de coordonner les autorités des États membres et d'États tiers dans leurs investigations et poursuites (**Titre I**). Par ailleurs, elle a promu l'investigation financière et l'a aidée à se développer (**Titre II**).

Titre I : Une coordination des organes d'investigation et de poursuite par l'Union européenne

L'Union européenne joue un rôle majeur dans la coordination des investigations et des poursuites par-delà les frontières internes, que ce soit par l'action de son législateur, lequel s'efforce d'harmoniser les législations et les politiques européennes (**Chapitre 1**) ou en fournissant des instruments de coordination et de coopération novateurs (**Chapitre 2**). C'est aussi un partenaire de choix pour les autorités de pays tiers dont le concours est nécessaire à la lutte contre le trafic de données personnelles (**Chapitre 3**).

Chapitre 1 : L'harmonisation des législations européennes

L'Union européenne a joué un rôle majeur dans la lutte contre la cybercriminalité, ces dernières années. Le législateur européen est mieux à même que les législateurs nationaux de réagir aux évolutions technologiques et sociales (*section 1*). Il a produit un droit européen révolutionnaire en matière de données personnelles (*section 2*) et il a amélioré l'approche financière de la cybercriminalité (*section 3*).

Section 1 : La position privilégiée du législateur européen face au trafic de données personnelles

Le législateur de l'Union européenne a une particulière légitimité pour intervenir en matière de protection des données personnelles. Les résultats de l'Eurobaromètre publiés récemment illustrent la volonté des peuples européens de lui confier la compétence en la matière. Comme l'indique le diagramme en annexe 48, une majorité des citoyens de l'UE préférerait que le problème soit traité à l'échelle de l'Union, plutôt qu'à l'échelle nationale. Parmi ceux-ci, comme l'illustre la carte en annexe 49, la population des membres fondateurs de l'UE manifeste un enthousiasme particulier (le Benelux, la France et l'Allemagne occupent cinq des sept premières places).[307]

Ce législateur s'est aussi souvent révélé plus efficace que les législateurs nationaux face aux nouvelles technologies. Peut-être y a-t-il à cela des raisons sociologiques. Le Parlement Européen est plus jeune que les parlements nationaux. La moyenne d'âge, en 2012, y était de 46 ans,[308] contre 59, par exemple, à l'Assemblée Nationale Française[309] et 61 pour le Sénat récemment élu.[310]

Peut-être aussi l'organisation du Parlement Européen, qui se repose massivement sur le lobbying,[311] a-t-elle encouragé l'intervention de la société civile dans un domaine où celle-ci a une expertise importante à offrir. D'ailleurs, la Commission a inséré dans son programme européen en matière de sécurité pour la période 2015-2020 l'objectif de développer le dialogue avec le secteur informatique pour lutter contre le terrorisme, la cybercriminalité et le crime organisé.[312] Ces partenariats ont donné le jour à des dialogues particulièrement fertiles avec les grandes entreprises informatiques dans le contexte de la lutte contre le terrorisme.[313]

307 Voir **Annexe 48 : Réponses des populations de l'UE (cercle extérieur) et française (intérieur) à la question de savoir quelle autorité devrait gérer la protection des données personnelles** et **Annexe 49 : Carte de l'Union européenne de la volonté des populations de confier la protection des données personnelles à l'Union européenne**.
308 Parlement Européen, *Questions fréquemment posées sur les députés européens et le Parlement européen*, 12 octobre 2012, 27 pp. [en ligne] (consulté le 20 août 2015) http://www.europarl.europa.eu/resources/library/media/20121018RES03126/20121018RES03126.pdf.
309 Assemblée Nationale, *Liste des députés répartis par âge*, Archive de la XIIIe législature, 19 juin 2012 [en ligne] (consulté le 20 août 2015) http://www.assemblee-nationale.fr/qui/xml/age.asp?legislature=13.
310 Sénat, *Renouvellement de Septembre 2014 Composition du Sénat (liste définitive) Par âge*, 2 octobre 2014 [en ligne] (consulté le 20 août 2015) http://www.senat.fr/senatoriales2014/listes/composition_par_age_apres_renouvellement_definitives_senat.pdf.
311 Commission Européenne, *Liste des lobbies enregistrés*, Registre de transparence (consulté le 20 août 2015) http://ec.europa.eu/transparencyregister/public/consultation/listlobbyists.do?locale=fr.
312 FLAUSCH Manon (traduction), *La Commission veut lutter en priorité contre le terrorisme et la cybercriminalité*, Euractiv [en ligne] (consulté le 20 août 2015) http://www.euractiv.fr/sections/leurope-dans-le-monde/la-commission-veut-lutter-en-priorite-contre-le-terrorisme-et-la.
313 Commission Européenne, *Déclaration commune Malmström - Alfano lors du dîner ministériel informel avec les entreprises technologiques*, 9 octobre 2014 [en ligne] (consulté le 20 août 2015) http://europa.eu/rapid/press-release_STATEMENT-14-304_en.htm.

La compétence du législateur de l'UE en matière de données personnelles est particulièrement légitime du fait de son adossement à la promotion des droits fondamentaux. Le droit de toute personne « *à la protection des données à caractère personnel la concernant* » est consacré dans la Charte des droits fondamentaux de l'UE, à un alinéa 1 de l'article 8 du chapitre II relatif aux libertés. Ce document, adopté suite au Conseil européen de Cologne de juin 1999, s'est vu conférer la même force juridique obligatoire que les traités en décembre 2009, à l'entrée en vigueur du traité de Lisbonne. S'il ne s'applique qu'aux institutions européennes dans l'exercice des compétences que les traités leur confèrent et aux pays de l'UE lorsqu'ils mettent en œuvre la législation de l'UE, ce texte constitue tout de même une déclaration de principes à la forte portée symbolique, entendue par les peuples de l'Union.

Cette déclaration est d'ailleurs reprise à l'alinéa 1 de l'article 16 du traité sur le fonctionnement de l'UE (TFUE), qui donne une compétence législative au Parlement européen et au Conseil pour fixer les règles relatives à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union, ainsi que par les États membres dans l'exercice d'activités qui relèvent du champ d'application du droit de l'Union, et à la libre circulation de ces données. Cette compétence est l'héritière de la compétence en matière d'harmonisation pour l'établissement et le fonctionnement du marché intérieur. Elle figure désormais à l'article 114, alinéa 1 du TFUE.

C'est plutôt la compétence du législateur européen en matière de coopération policière qui nous intéresse ici. L'article 87 du TFUE permet à ce législateur d'intervenir en matière de coopération policière entre autorités compétentes des États membres (services de police, services des douanes et autres services répressifs spécialisés dans les domaines de la prévention ou de la détection des infractions pénales et des enquêtes en la matière). Alors que les coopérations opérationnelles restent du domaine de la procédure législative spéciale, la procédure législative ordinaire s'applique en matière de collecte, de stockage, de traitement, d'analyse et d'échange d'informations pertinentes, de soutien à la formation de personnel, d'échange de personnel, d'équipements et de recherche en criminalistique, de techniques communes d'enquête concernant la détection de formes graves de criminalité organisée.

L'article 88 traite de l'Office européen de police (Europol), le principal instrument de la coopération policière. D'autres organes ont été créés, dont le Collège européen de Police (CEPOL) devenu une agence de l'Union européenne suite à la décision 2005/681/JAI du Conseil du 20 septembre 2005 et le Comité permanent de coopération opérationnelle en matière de sécurité intérieure (COSI) constitué officiellement par la décision du Conseil du 25 février 2010.

Par ailleurs, dans une perspective de judiciarisation des enquêtes transnationales dans l'UE, l'article 85 permet au Parlement et au Conseil de fixer la mission d'une unité de coopération judiciaire de l'Union européenne (Eurojust) pour « *appuyer et renforcer la coordination et la coopération entre les autorités nationales chargées des enquêtes et des poursuites relatives à la criminalité grave affectant deux ou plusieurs États membres ou exigeant une poursuite sur des bases communes, sur la base des opérations effectuées et des informations fournies par les autorités des États membres et par Europol.* »

La législation de l'Union trace donc un cadre riche permettant des enquêtes coordonnées. Elle est également novatrice en matière de protection des données personnelles. Bien que ces dispositions ne traitent aucunement des aspects pénaux et n'intéressent donc pas directement notre étude, elles ne peuvent manquer d'avoir un impact sur la conception européenne de la cybercriminalité.

Section 2 : La rénovation de la protection des données personnelles par le législateur européen

L'UE a légiféré précocement sur la question des données personnelles par la directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, texte de référence au niveau européen. Elle s'efforce d'établir un équilibre entre protection de la vie privée des personnes et libre circulation des données à caractère personnel au sein de l'UE. Elle ne concerne pratiquement que le traitement privé (sauf sécurité publique, défense ou sûreté de l'État). Elle nous intéresse surtout parce qu'elle donne à la personne concernée un certain nombre de droits. Elle impose aussi des responsabilités aux organisations traitant des données personnelles, dont celui d'assurer la sécurité des données contre la destruction illicite, la perte accidentelle, la diffusion ou l'accès non autorisés par des mesures techniques et d'organisation appropriées.[314] Elle crée aussi 28 autorités de contrôle en matière de données personnelles (article 28), réunies dans un groupe européen purement consultatif (articles 29 et 30).

Comme nous l'avons expliqué plus haut, la définition des données personnelles que pose cette directive n'a pas été transposée de façon claire et détaillée par les États. La réforme du dispositif en cours ne la précise pas davantage, l'actualisant seulement (avec la prise en compte des données génétiques ou biométriques, par exemple). Elle ne développe pas non plus le volet pénal du trafic,

314 Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, Chapitre II (« Conditions générales de licéité des traitements de données à caractère personnel »), Section VIII.

qui a seulement été évoqué durant les travaux de rédaction sous l'angle de la responsabilité des acteurs du traitement des données face aux fuites. Les nouvelles dispositions devraient obliger les entreprises à renforcer leurs mesures de sécurité pour prévenir ces fuites, mais aussi à notifier les personnes concernées et les autorités nationales de leur existence. Cette prise en compte transparaît dans la définition de la violation de données personnelles (« *violation de la sécurité entraînant de manière accidentelle ou illicite la destruction, la perte, l'altération, la divulgation ou la consultation non autorisées de données à caractère personnel transmises, conservées ou traitées d'une autre manière* »).[315]

Dans son programme en matière de sécurité,[316] la Commission a rappelé que le législateur de l'UE avait conçu tout un dispositif en matière de sécurité, surtout par la proposition de directive concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et de l'information dans l'Union.[317] Cette proposition encouragerait les États membres à améliorer leur niveau de préparation et de coopération mutuelle, et les opérateurs Internet à adopter les mesures appropriées pour gérer les risques de sécurité et signaler les incidents graves aux autorités nationales compétentes.

Elle compléterait la directive 2013/40/UE du 12 août 2013 relative aux attaques contre les systèmes d'information, laquelle visait le rapprochement des droits pénaux nationaux en définissant les infractions pénales (l'accès illégal à des systèmes d'information, l'atteinte illégale à l'intégrité d'un système ou de données, leur interception illégale, la mise à disposition intentionnelle d'un outil les permettant, l'incitation, la participation, la complicité et la tentative) et les sanctions applicables,[318] en renforçant la coopération entre les autorités compétentes et avec les agences et organes spécialisés compétents de l'Union. Sans définir la cybercriminalité, cette directive mettait en place un arsenal d'infractions complet. Bien que ces définitions prennent le problème des données personnelles en compte, elles ne s'y limitent pas. Les sanctions n'étaient pas fixées explicitement dans la décision-cadre 2001/413/JAI du Conseil du 28 mai 2001 concernant la lutte contre la fraude et la contrefaçon des moyens de paiement autres que les espèces.

Les rapports de transposition, comme le programme, signalaient les réticences des États à

315 Commission Européenne, *Communication COM/2012/09 final Protection de la vie privée dans un monde en réseau Un cadre européen relatif à la protection des données, adapté aux défis du 21e siècle*, 25 janvier 2012.
316 Commission Européenne, *Communication COM(2015) 185 final Le programme européen en matière de sécurité*, 28 avril 2015.
317 Commission Européenne, *Communication COM(2013) 48 final Proposition de directive concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et de l'information dans l'Union*, 7 février 2013.
318 Les quatre premiers comportements font encourir une peine d'emprisonnement maximale d'au moins deux ans, poussée à cinq ans dans le cadre d'une entreprise criminelle ou du système d'information d'une infrastructure critique. Les trois derniers entraîneraient une peine d'emprisonnement d'au moins trois ans.

transposer les dispositions facilitant la coopération en limitant leur compétence.[319]

Le législateur de l'UE n'a donc pas réussi à réaliser l'harmonisation des infractions et des sanctions pénales en matière de trafic de données personnelles. Il a toutefois mené une action dans le cadre de la lutte contre le blanchiment d'argent. Les institutions de l'UE ont fait la promotion de l'investigation financière.

Section 3 : La prise en compte de l'aspect financier de la criminalité par le législateur européen

Le 20 mai 2015, l'UE a adopté ce qui a été qualifié de « pack anti-blanchiment », c'est-à-dire un règlement et une directive destinés à durcir les règles européennes en matière de blanchiment de capitaux et de financement du terrorisme.[320] Ces textes mettent en œuvre les recommandations du Groupe d'Action FInancière (GAFI) et s'efforcent de répondre aux évolutions de la technologie.

Le propos du règlement est surtout de renforcer la traçabilité des transferts de fonds par la transmission de davantage d'informations sur le donneur d'ordre ou le bénéficiaire, en plus du signalement.

La directive de 2015, la quatrième sur le sujet, élargit le champ des directives précédentes. Son article 2, alinéa 3.f) étend par exemple l'application de ses dispositions, remplaçant une disposition initiale qui ne visait que les casinos à tous les prestataires de services de jeux d'argent et de hasard. Son alinéa e) abaisse par ailleurs le seuil de paiement en espèces à partir duquel les négociants en biens entrent dans le champ d'application, de 15.000 à 10.000 euros.

Elle donne également une prise aux forces de l'ordre sur toute activité de blanchiment d'argent menée par le crime organisé, en rendant obligatoire la création d'infractions fiscales pénales liées aux impôts directs et indirects.[321]

319 Commission Européenne, Communication COM/2006/0065 final, *Rapport de la Commission - Deuxième rapport fondé sur l'article 14 de la décision-cadre du Conseil du 28 mai 2001 concernant la lutte contre la fraude et la contrefaçon des moyens de paiement autres que les espèces {SEC(2006) 188}* : L'article 9 prévoit des critères d'attribution de la compétence juridictionnelle (faits constitutifs sur son territoire, commis par ses ressortissants ou au bénéfice d'une personne morale ayant son siège sur le territoire de l'État membre compétent.

320 *Directive (UE) 2015/849 du Parlement Européen et du Conseil du 20 mai 2015 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme, modifiant le règlement (UE) n° 648/2012 du Parlement européen et du Conseil et abrogeant la directive 2005/60/CE du Parlement européen et du Conseil*, *Directive 2006/70/CE de la Commission (Texte présentant de l'intérêt pour l'EEE)* et *Règlement (UE) 2015/847 du Parlement européen et du Conseil du 20 mai 2015 sur les informations accompagnant les transferts de fonds et abrogeant le règlement (CE) n° 1781/2006 (Texte présentant de l'intérêt pour l'EEE)*.

321 Cabinet OPF Partners, *Lutte contre le blanchiment et le financement du terrorisme: deux nouveaux instruments européens*, Document de travail, 9 juin 2015 [en ligne] (consulté le 20 août 2015) http://www.opf-partners.com/wp-

La section 2 de la directive prévoit d'étendre l'approche par les risques au niveau international : la Commission devra coordonner l'évaluation du blanchiment de capitaux et le risque de financement du terrorisme qui touchent le marché intérieur et concernent les activités transfrontalières. L'approche par les risques est en effet centrale dans le traitement par les enquêteurs financiers des nouveaux instruments du blanchiment d'argent (et en particulier du paiement). Par exemple, les services de jeux d'argent et de hasard seront soumis à des exigences différentes suivant les risques qu'ils présentent, les plus à risque devant exercer une diligence raisonnable pour les transactions de 2.000 euros ou plus et les moins à risque pouvant en être exemptés.[322]

Cette approche par les risques va profondément affecter les méthodes de travail de l'enquêteur financier européen et la façon dont Europol coordonnera l'espace de liberté, de sécurité et de justice.

content/uploads/2015/06/Lutte-contre-le-blanchiment-Deux-nouveaux-instruments-europ%C3%A9ens_20150609.pdf.

322 QUILLÉROU Charline, *Quatrième directive anti-blanchiment : l'Union européenne renforce son arsenal pour lutter contre le blanchiment de capitaux et le financement du terrorisme. L'Union au premier plan dans la lutte contre le blanchiment et le financement du terrorisme?*, Portail Europe liberté sécurité et justice, 17 juin 2015 [en ligne] (consulté le 20 août 2015) http://europe-liberte-securite-justice.org/2015/06/17/quatrieme-directive-anti-blanchiment-lunion-europeenne-renforce-son-arsenal-pour-lutter-contre-le-blanchiment-de-capitaux-et-le-financement-du-terrorisme-lunion-au-premier-plan-da/.

Chapitre 2 : Un espace de liberté, de sécurité et de justice qui se dote d'outils de coordination et de coopération novateurs

L'Union européenne, cet espace de liberté, de sécurité et de justice, fournit aux services d'enquête et de poursuite de nombreux moyens de se coordonner et de coopérer. Les équipes communes d'enquête permettent de coordonner les enquêtes et les poursuites (*section 1*). Europol joue un rôle en tant qu'analyste et coordinateur des informations produites par les investigations financières, ainsi que des opérations des polices nationales (*section 2*). Le mandat d'arrêt européen facilite la remise des personnes impliquées dans la cybercriminalité (*section 3*).

Section 1 : Les nouveaux moyens d'investigation fournis par l'Union européenne

Nous avons déjà expliqué que les États membres de l'UE menaient des opérations conjointes avec des États tiers, comme dans l'opération « *Blackshades* ». L'Union met à la disposition de ses membres un outil très intéressant, l'équipe commune d'enquête.[323]

Il s'agit d'une équipe d'enquêteurs et d'autorités judiciaires de deux États ou plus, travaillant ensemble, avec l'autorité de membres des forces de l'ordre et dans le respect du droit. L'objectif des équipes communes était de renforcer la lutte contre la criminalité organisée. Elles devaient être créées pour un dossier déterminé et une durée limitée.

L'intérêt de cet instrument est que les autorités appropriées d'États tiers peuvent participer au fonctionnement d'une telle équipe, même sans avoir le statut de membres. Il faut pour cela qu'il existe une base juridique, qu'il s'agisse d'un instrument juridique international, d'un accord bilatéral, d'un accord multilatéral ou d'une législation nationale. De tels textes ont déjà été signés, qui sont applicables au trafic de données personnelles en ligne, comme le deuxième Protocole additionnel à la Convention d'entraide judiciaire en matière pénale du Conseil de l'Europe du 20 avril 1959 (article 20), la Convention sur la coopération policière pour l'Europe du sud-est, du 5 mai 2006 (article 27) ou l'accord entre l'Union européenne et les États-Unis d'Amérique en matière d'entraide judiciaire (article 5).

Les membres de l'équipe exécutent leur mission dans le respect des conditions fixées par leurs

323 L'équipe commune d'enquête a été mise en place par la Convention relative à l'entraide judiciaire en matière pénale, signée à Bruxelles, le 29 mai 2000 entre les États membres de l'Union européenne. En France, le dispositif a été transposé aux articles 695-2 et 695-3 du Code de procédure pénale par la loi n° 2004-204 du 9 mars 2004 portant adaptation de la justice aux évolutions de la criminalité.

propres autorités dans l'accord portant création de l'équipe commune d'enquête et le membre sur le territoire duquel l'équipe mène une action la réalise dans le respect du droit national.

Eurojust et Europol peuvent participer aux équipes communes d'enquête, conformément à l'article 1er, paragraphe 12, de la décision-cadre. Leur association n'est pas obligatoire mais elle est encouragée par les modalités de financement et d'équipement des équipes. Les deux agences ont une plus-value à apporter. Europol a gagné une certaine notoriété dans le domaine de la cybercriminalité, qui fait de son expertise une valeur ajoutée.[324]

Néanmoins, Europol intervient aujourd'hui rarement sans Eurojust, au point d'avoir conclu un *Accord entre Eurojust et Europol pour le placement temporaire d'un représentant d'Eurojust au Centre européen de lutte contre la cybercriminalité (EC3)*, afin de faciliter l'échange d'informations et d'assurer la recevabilité des éléments de preuve dans les procédures judiciaires.[325] Cette capacité a été renforcée par le placement de magistrats spécialisés d'États tiers auprès de l'agence.[326]

D'après l'article 88 du TFUE, l'agence Europol est un instrument essentiel de la coopération policière au sein de l'UE. Sa première mission est d'appuyer et de renforcer l'action des autorités policières et des autres services répressifs des États membres. Elle doit aussi appuyer et renforcer leur collaboration dans la prévention de la criminalité grave affectant au moins deux États membres, du terrorisme et des formes de criminalité portant atteinte à un intérêt commun qui fait l'objet d'une politique de l'Union, ainsi que la lutte contre ceux-ci.

L'alinéa 2 de l'article délimite les tâches d'Europol, y incluant la collecte, le stockage, le traitement, l'analyse et l'échange des informations, transmises notamment par les autorités des États membres ou de pays ou instances tiers, ainsi que la coordination, l'organisation et la réalisation d'enquêtes et d'actions opérationnelles. Néanmoins, selon l'alinéa 3, celles-ci doivent être réalisées en liaison et en accord avec les autorités du ou des États membres dont le territoire est concerné et Europol ne peut réaliser aucune mesure de contrainte. Mais ses compétences opérationnelles s'étendent progressivement, comme le montre l'acte du Conseil du 28 novembre 2002 qui lui permet de participer à des équipes communes d'enquête et de demander aux États membres d'ouvrir des enquêtes pénales. Il s'efforce aussi d'accroître ses capacités d'analyse, comme l'illustre la création, en janvier 2013, du Centre européen de lutte contre la cybercriminalité (EC3).

324 Conseil de l'Union européenne, *Manuel sur les équipes communes d'enquête*, Note du Secrétariat général du Conseil aux délégations, n°13598/09 COPEN 178 ENFOPOL 218 EUROJUST 55 EJN 35, Bruxelles, 4 novembre 2011.
325 Eurojust, *Rapport annuel pour 2014*, La Haye, Pays-Bas, 2015, 33 p..
326 Les 15 et 16 septembre dernier, l'avocate générale du département de la justice américain a annoncé la nommination d'un procureur américain pour la cybercriminalité auprès d'Eurojust et d'EC3: Eurojust, « *US Attorney General Lynch announces Cyber Prosecutor at Eurojust* », La Haye, 16 septembre 2015 [en ligne] (consulté le 27 septembre 2015) http://www.eurojust.europa.eu/press/PressReleases/Pages/2015/2015-09-16.aspx.

Section 2 : La contribution d'Europol sur les plans analytiques et opérationnels

La création du centre EC3 a consacré l'expertise informatique d'Europol, qui exprime à présent sa volonté de fournir une expertise informatique aux autorités nationales, en trois volets : l'établissement de stratégies, la recherche et le développement et la formation des forces de l'ordre.[327] Parmi les trois spécialités du centre, outre les formes de cybercriminalité qui causent de réels dommages à la victime (à l'exemple de la pédopornographie) et celles qui pourraient porter atteinte aux infrastructures et systèmes d'informations cruciaux dans l'Union européenne, EC3 concentre ses efforts sur les groupes organisés, particulièrement ceux générant de larges profits. Le trafic de données personnelles en ligne entre précisément dans cette catégorie.

Le centre EC3 participe à l'effort des polices nationales en rassemblant les informations sur ces crimes et criminels, en fournissant aux États membres une analyse opérationnelle, en coordonnant leurs opérations et investigations et en mettant en commun les diverses expertises développées, en faisant le lien entre les forces de l'ordre et le secteur privé, notamment académique, en assistant les États membres dans l'entraînement et l'équipement des autorités compétentes, en fournissant des capacités d'analyse forensique spécialisées pour assister l'investigation et les opérations et en représentant les forces de l'ordre à l'échelle de l'UE (la recherche, la gouvernance numérique et le développement de politiques).

La connexion de l'EC3 avec la société civile est si étroite qu'elle a acquis une dimension organisationnelle. Le Conseil de programmation (*Programme Board*) est la structure de l'EC3 qui se charge de bâtir des partenariats, des partages de responsabilités et des collaborations. Il a créé des Groupes consultatifs (*Advisory Groups*), qui encouragent la coopération avec des partenaires n'appartenant pas aux forces de l'ordre. Les groupes « Sécurité Internet » et « Services Financiers » assurent la liaison avec les leaders de ces deux domaines.

Le centre est déjà opérationnel et a permis de coordonner des opérations intra-UE, aussi bien qu'entre les autorités des États membres et celles d'États tiers, tant en poursuivant des objectifs précis concernant un groupe de cyberdélinquants définis qu'en menant des formes de cyberpatrouilles dans le *deep web* et sur le réseau TOR.[328]

327 *Combatting crime in a digital age*, Europol, EC3, 25 avril 2013 [en ligne] (consulté le 20 août 2015) http://www.anacom.pt/streaming/Benoit_Godart.pdf?contentId=1176117&field=ATTACHED_FILE.

328 *Global action against dark markets on Tor network*, Commission Européenne, Nouvelles, 7 novembre 2014 [en ligne] (consulté le 20 août 2015) http://ec.europa.eu/dgs/home-affairs/what-is-new/news/news/2014/20141107_01_en.htm et 25 février 2015, *Botnet taken down through international law enforcement cooperation* [en ligne] (consulté le 20 août 2015) http://ec.europa.eu/dgs/home-affairs/what-is-

Il offre donc une expertise purement informatique, mais manifeste aussi une conscience des formes d'organisation des trafiquants de données personnelles en ligne. Il a publié un premier rapport d'analyse des menaces informatiques en septembre 2014 et prévoit d'en publier une version actualisée en septembre prochain. Le rapport iOCTA (*Internet Organised Crime Threat Assessment*) apporte une analyse nécessaire.[329] En effet, la doctrine devait s'appuyer sur l'analyse d'acteurs privés, souvent des firmes de cybersécurité. Elle constitue d'ailleurs l'échine de cette étude, ce qui n'est pas sans amener des interrogations quant à la neutralité des informations et leur fiabilité.

Il est aussi positif que l'EC3 fasse preuve d'une certaine discrimination face aux techniques employées par les pirates, comme ses activités de cyberpatrouille ont pu l'illustrer. Il limite son intervention aux activités manifestement nuisibles (d'où son aire d'expertise). Il encourage l'imitation par les autorités nationales de cette attitude proactive, coordonnant les arrestations, les perquisitions et les poursuites à travers tous les pays concernés par ces coups de filet.[330]

La nature transnationale des activités cybercriminelles implique qu'elles ne puissent être contrées que par une excellente coordination, tant des polices que des autorités judiciaires des différents États, par exemple quant à l'extradition.

Section 3 : La désuétude du système de l'extradition à l'intérieur de l'Union européenne

Au lendemain du 11 septembre, l'UE s'est dotée d'un instrument qui simplifie considérablement la remise des personnes, le mandat d'arrêt européen, créé par la décision-cadre n°2002/584/JAI du 13 juin 2002. Son article 2, alinéa 2, supprime la condition de double incrimination pour un certain nombre d'infractions, si elles sont punies dans l'État membre d'émission d'une peine ou d'une mesure de sûreté privatives de liberté d'un maximum d'au moins trois ans. Au moins huit d'entre elles peuvent s'insérer dans le trafic de données personnelles, tels que nous l'avons défini : la participation à une organisation criminelle, la fraude, le blanchiment du produit du crime, la cybercriminalité, le racket et l'extorsion de fonds, la contrefaçon et le piratage de produits, la falsification de documents administratifs et le trafic de faux, et la falsification de moyens de paiement.

Le mandat d'arrêt européen est une concrétisation du principe de reconnaissance mutuelle, selon

new/news/news/2015/20150225_02_en.htm.
329 *The Internet Organised Crime Threat Assessment (iOCTA) 2014*, EC3, Europol, 2014, 92 pp..
330 Comme il l'a fait dans l'opération *Mousetrap*, citée plus haut.

lequel les autorités d'un État membre traitent les décisions de toute autorité d'un État membre comme si elles émanaient d'une autorité nationale. Ce principe a posé un problème de conformité au principe de légalité. La CJUE a dû déterminer si l'imprécision des trente infractions pour lesquelles la condition de double incrimination est supprimée conduisait à une violation des principes de légalité, d'égalité et de non-discrimination. Ne s'agissant pas d'une harmonisation, la possibilité d'une violation a été écartée.[331]

Le principe de reconnaissance mutuelle apparaît comme un instrument intéressant dans la perspective d'une lutte au niveau européen contre les trafiquants de données personnelles en ligne. L'exemple du mandat d'arrêt européen montre qu'il n'est cependant pas sans implications du point de vue des droits de l'Homme.

Les articles 3 et 4 de la décision-cadre aménagent trois motifs de non-exécution obligatoire du mandat d'arrêt européen[332] et sept facultatifs[333] mais les droits fondamentaux ne priment jamais sur la reconnaissance mutuelle en-dehors de ces dix dispositions.[334] Même les organes de l'UE ont souligné la nécessité d'insérer une clause de respect des droits fondamentaux dans la décision-cadre. La Commission, dans ses rapports de suivi, recommande au législateur européen de consacrer les standards du droit pénal.[335] La Commission des libertés, de la justice et des affaires intérieures (LIBE) du Parlement Européen est plutôt favorable à la création d'un quatrième motif de refus contraignant, l'incompatibilité avec les obligations de l'État membre d'exécution en termes de droits fondamentaux.[336]

Le conflit entre les droits fondamentaux et l'efficacité de la coopération policière et judiciaire devrait se poser en des termes plus pressants s'agissant de l'établissement de partenariats internationaux de lutte contre la cybercriminalité par l'Union européenne.

331 CJCE, Affaire C-303/05, 3 mai 2007, *Advocaten voor de Wereld*.
332 L'amnistie de l'infraction dans l'État d'exécution, l'application du principe de *ne bis in idem* ou la minorité pénale dans l'État d'exécution.
333 La double incrimination pour les infractions non inscrites sur la liste, l'existence de poursuites pour les mêmes faits dans l'État d'exécution, le classement sans suite ou le non lieu dans l'État d'exécution, la prescription dans l'État d'exécution, l'existence d'une décision définitive rendue par un État tiers, l'exécution de la peine dans l'État de nationalité et la localisation des faits sur le territoire de l'État d'exécution ou localisation des faits hors du territoire de l'État d'émission, l'État d'exécution n'autorisant pas les poursuites pour les mêmes infractions commises hors de son territoire.
334 Selon l'arrêt CJUE, Affaire C-396/11, 29 janvier 2013, *Radu*, l'émission d'un mandat d'arrêt ne nécessite pas d'avoir entendu la personne recherchée. Selon l'arrêt CJUE, Affaire C-399/11, 26 février 2013, *Melloni*, l'exécution d'un mandat d'arrêt européen ne saurait être refusée pour incompatibilité avec les droits fondamentaux garantis par la Constitution de l'État requis.
335 Commission Européenne, Bruxelles, 11 avril 2011, Communication COM(2011) 175 final, *Rapport sur la mise en œuvre depuis 2007 de la décision-cadre du conseil du 13 juin 2002 sur le mandat d'arrêt européen et les procédures de remise entre États membres {SEC(2011) 430 final}*.
336 LUDFORD Sarah, *Rapport A7-0039/2014 contenant des recommandations à la Commission sur la révision du mandat d'arrêt européen*, Commission des libertés, de la justice et des affaires intérieures, Parlement Européen, 22 janvier 2014.

Chapitre 3 : Une gestion des partenariats internationaux de lutte contre la cybercriminalité par l'Union européenne

L'Union européenne ne s'est pas contentée de faciliter la coopération policière et judiciaire à l'intérieur de ses frontières, elle s'efforce également d'étendre les partenariats entre forces de police et juridictions au niveau international. Après la généralisation de la remise de personnes entre États membres, elle négocie désormais des accords d'extradition vers ou depuis les États tiers (*section 1*). Il va en effet lui falloir mettre en place de véritables partenariats internationaux de lutte contre le trafic de données personnelles (*section 2*) mais, pour donner une effectivité à cette lutte, elle devra aussi faciliter l'exécution des décisions de justice en aménageant une responsabilité des opérateurs Internet compatible avec les impératifs en termes de droits de l'Homme (*section 3*).

Section 1 : La facilitation de l'extradition vers et depuis les États tiers partenaires en matière de cybercriminalité

Avant toute autre chose, il faut signaler que les accords d'extradition entre États européens ont historiquement d'abord été passés au sein du Conseil de l'Europe. Le premier de ces textes assurant et simplifiant l'extradition est la Convention européenne d'extradition, signée le 13 décembre 1957 et entrée en vigueur le 18 avril 1960, puis additionnée de quatre protocoles.

Ce traité est d'une toute particulière importance, ne serait-ce que par le nombre de ses parties, parmi lesquelles on trouve des membres du Conseil de l'Europe qui n'appartiennent pas à l'Union. La Russie, la Turquie et l'Ukraine apparaissent ainsi incontournables. Il s'applique aussi à trois États non-européens, l'Afrique du Sud, la Corée et Israël.

La procédure applicable aux demandes dans le cadre de cette convention respecte le principe de la territorialité pénale et les demandes sont toujours transmises par voie de canaux diplomatiques (article 12) mais la décision d'extrader revient aux autorités judiciaires centrales. Par ailleurs, le champ de la convention est très large : seules les infractions politiques et fiscales sont exclues et une peine privative de liberté d'un an minimum doit être encourue. Les infractions informatiques entrent donc tout à fait dans ce champ.

Néanmoins, l'Union n'est concernée par ce texte que par le biais de ses États membres. Beaucoup plus intéressante est sa capacité à être elle-même partie à une convention d'extradition.

La principale convention d'extradition négociée à l'échelle de l'UE est l'accord de 2003 entre l'Union européenne et les États-Unis d'Amérique en matière d'extradition. Son intérêt tient essentiellement à l'article 3, alinéa 1 qui ventile son champ d'application par rapport aux traités bilatéraux d'extradition conclus par les États membres. Il s'applique en lieu et place de ceux-ci quant à la définition des infractions pouvant donner lieu à extradition (article 4), les modalités de transmission et d'authentification des documents (article 5). Il pourra au contraire seulement suppléer l'absence de traité ou leur silence quant aux dispositions sur la transmission des demandes d'arrestation provisoire (article 6), la transmission de documents à la suite d'une arrestation provisoire (article 7), les compléments d'informations (article 8), la remise temporaire (article 9), les demandes d'extradition ou de remise présentées par plusieurs États (article 10), les procédures d'extradition simplifiées (article 11), le transit (article 12), la peine de mort (article 13) et la présence d'informations sensibles dans une demande (article 14).

L'article 4, donc, qui fixe le champ des infractions pouvant donner lieu à extradition, est d'une particulière importance. Or, il est très inclusif, permettant l'extradition face aux infractions punissables, en vertu du droit de l'État requérant et de celui de l'État requis, d'une peine privative de liberté d'une durée maximale de plus d'un an ou d'une peine plus sévère, pour les tentatives de commission de telles infractions, les conspirations à cet effet et participations à de telles infractions.

Naturellement, les conditions de double incrimination, de compétence fédérale côté américain, sont maintenues, de même que celle selon laquelle l'infraction commise hors du territoire de l'État requérant n'entraîne automatiquement l'extradition que si le droit de l'État requis prévoit des sanctions pour des faits commis hors de son territoire dans des circonstances analogues.

Les États membres se sont en particulier réjouis de la formulation de l'article 13 sur la peine de mort, qui permet le conditionnement de l'extradition à la non-prononciation ou la non-exécution de la peine de mort. Si une disposition similaire existait déjà dans l'accord d'extradition de 1996 entre la France et les États-Unis, il n'y avait pas de hiérarchisation de ces deux conditions, la seconde n'intervenant qu'en cas d'impossibilité procédurale de la première. La France a aussi été satisfaite du traitement de la question des « juridictions d'exception » américaine par la convention, laquelle permet, par le renvoi aux accords bilatéraux, de faire jouer la plupart des motifs de refus d'extradition, notamment les infractions politiques et la remise des nationaux, ainsi que la violation éventuelle des « principes constitutionnels de l'État requis ».[337]

Les discussions les plus vives ont porté sur l'article 10, qui fixe les priorités à établir en matière

337 FAUCHON Pierre, Communication E 2210 sur les projets d'accords entre l'Union européenne et les États-Unis d'Amérique en matière d'extradition et d'entraide judiciaire, Sénat Français, Justice et affaires intérieures, 1er avril 2003 [en ligne] (consulté le 20 août 2015) http://www.senat.fr/ue/pac/E2210.html.

d'extradition. Un débat porte en particulier sur son alinéa 2. Il assimile le mandat d'arrêt européen à une extradition mais il ne crée de priorité pour la remise entre États membres au cas où le mandat soit en concurrence avec une demande d'extradition des États-Unis. Par ailleurs, malgré les réticences des États-Unis, les notes explicatives rappellent que les demandes de la Cour Pénale Internationale (CPI) conservent la priorité sur toute autre demande d'extradition.

L'accord de 2003 entre l'Union européenne et les États-Unis d'Amérique en matière d'extradition s'est doublé d'un accord d'entraide judiciaire, également signé en juin 2003 à Washington.[338]

Section 2 : La capacité de l'Union européenne à établir des coopérations internationales d'entraide dans la lutte contre le trafic de données personnelles

L'UE est signataire de plusieurs accords d'entraide judiciaire qui impactent notamment la coordination internationale de la lutte contre le trafic de données personnelles en ligne. La promotion de tels accords s'appuie sur les activités de l'Union dans les fora internationaux sur la cybercriminalité.

L'accord avec les États-Unis prend globalement la même forme que l'accord d'extradition, s'efforçant d'améliorer la lutte contre la criminalité internationale et de faire converger les accords d'extradition et d'entraide des États membres, tout en renforçant les garanties des accusés, en confirmant celles énoncées dans les accords bilatéraux des États membres et en y ajoutant celles qui découlent de la législation européenne, notamment de la Charte des droits fondamentaux.

Après cet accord et ceux avec l'Australie ou encore la Norvège et l'Islande,[339] fin 2009, l'UE a signé avec le Japon son premier accord d'entraide pénale complètement autonome de tout accord passé avec cet État par les États membres. L'article 3 de celui-ci fixe le champ de l'entraide, lequel est délimité dans un souci d'efficacité. Il inclut entre autres l'obtention d'éléments, y compris grâce à l'exécution d'une perquisition ou d'une saisie, de relevés, de documents ou de rapports concernant des comptes bancaires, la localisation ou l'identification de personnes, d'éléments ou de lieux, la participation à des procédures liées au gel ou à la saisie et à la confiscation de produits ou

338 États-Unis, Union européenne, *Accord entre l'Union européenne et les États-Unis d'Amérique en matière d'entraide judiciaire* et *Accord entre l'Union européenne et les États-Unis d'Amérique en matière d'extradition*, Décision 2009/820/PESC, signé à Washington le 25 juin 2003 et en vigueur le 1er février 2010.
339 Australie, Union européenne, texte E 5038, *Accord avec l'Australie sur le transfert de données PNR*, Islande, Norvège, Union européenne, texte E 5041, *Accord avec la Norvège et l'Islande sur l'entraide judiciaire en matière pénale* et texte E 5042, *Accord avec la Norvège et l'Islande sur la procédure de remise.*

d'instruments ou encore toute autre entraide autorisée en vertu du droit de l'État requis et convenue entre un État membre et le Japon. La révolution concerne la forme des demandes d'entraide, qui devraient être écrites mais pourraient transiter par tout autre moyen de communication fiable en cas d'urgence, conformément à l'article 8 de l'accord.[340]

La passation de tels accords va être promue au sein des fora internationaux ou constituer une première étape de la création de ceux-ci. Ainsi, la coopération entre les États-Unis et l'UE s'est dotée d'un groupe de travail permanent sur la cybersécurité et la cybercriminalité. Ce groupe institutionnalise la vision à long terme de la lutte contre ce type de crimes. Créé lors du sommet États-Unis - UE de novembre 2010, il a participé au rapprochement des autorités de ces deux régions, avec des concrétisations dès la table ronde de 2011.

Parmi ces concrétisations, il faut citer la création d'une alliance globale contre l'abus sexuel des enfants en ligne (« *Global Alliance against Child Sexual Abuse Online* »).[341] L'initiative conjointe de décembre 2012 qui lui a donné le jour est conforme à l'autre modèle de partenariats internationaux contre la cybercriminalité, avec un objet plus étroit mais une base de participation plus large. En effet, elle intègre 53 États, dont des membres d'horizons aussi variés que le Ghana, la Thaïlande, les membres de l'Union européenne ou la Serbie. Tous s'engagent à atteindre quatre objectifs politiques, liées à la lutte contre la pédopornographie.[342]

L'Union européenne va aussi s'imposer dans les fora internationaux créés par d'autres organisations internationales, comme l'OCDE, les Nations Unies, Union Internationale des Télécommunications (ITU), l'OSCE, etc. Même Interpol a complété son assistance opérationnelle par la tenue de conférences régulières entre partenaires impliqués dans la lutte contre la cybercriminalité.[343]

L'UE a aussi tout particulièrement collaboré avec le Conseil de l'Europe dans le cadre de l'implémentation de sa Convention sur la cybercriminalité, menant entre autres depuis le début des années 2000 un projet visant à améliorer les législations, tant des États membres des deux

340 Japon, Union européenne, *Accord entre l'Union européenne et le japon relatif à l'entraide en matière pénale*, Décision 2010/616/UE, signé à Bruxelles le 3 novembre 2009, à Tokyo le 15 décembre 2009 et en vigueur le 2 janvier 2011.
341 Service européen pour l'action extérieure (SEAE, *EU-US cooperation on cyber security and cyberspace*, Factsheet 140326/01, Bruxelles, 26 mars 2014, 3 pp. [en ligne] (consulté le 20 août 2015) http://www.eeas.europa.eu/statements/docs/2014/140326_01_en.pdf.
342 Commission Européenne, Rapport Affaires internes, décembre 2013, *Global Alliance against Child Sexual Abuse Online*, 28 pp. [en ligne] (consulté le 20 août 2015) http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/global-alliance-against-child-abuse/docs/global_alliance_report_201312_en.pdf.
343 Interpol, *Europol-INTERPOL Cybercrime Conference 30 September to 2 October 2015*, La Haye, Pays-Bas, Nouvelles [en ligne] (consulté le 20 août 2015) http://www.interpol.int/fr/News-and-media/Events/2015/Europol-INTERPOL-Cybercrime-Conference/Europol-INTERPOL-Cybercrime-Conference.

organisations que d'États tiers – d'Europe de l'Est, d'Afrique et d'Asie, justement – et la coopération opérationnelle avec ceux-ci.[344]

La construction de partenariats viables avec l'ensemble de ces interlocuteurs internationaux, États ou organisations, suppose néanmoins le respect des droits fondamentaux.

Section 3 : La nécessité d'aménager une responsabilité des opérateurs Internet viable à l'échelle internationale

Internet implique surtout deux des droits fondamentaux universellement consacrés dans la Déclaration universelle des droits de l'Homme : le droit à la vie privée (article 12) et la liberté d'expression (article 19). L'UE et ses partenaires européens ont exprimé leur attachement à ces deux principes en signant la Convention européenne des droits de l'Homme articles 8 et 10.

Le texte les limite cependant. L'ingérence des autorités publiques est possible, dans la mesure où elle est prévue par la loi et constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale ou à la protection des droits et libertés d'autrui. La Charte des droits fondamentaux ne réitère pas ces limites à l'échelle des États membres, élargissant plutôt ces droits et libertés (articles 7, 8 et 11), ce qui explique que le système interne de l'UE assure déjà une certaine conformité aux droits fondamentaux.

Une directive de 2006 obligeait les FSI[345] à conserver un certain nombre de données sur les services de communication utiles aux enquêtes pendant un minimum de six mois et un maximum de deux ans.[346] En 2008, la CEDH avait déjà affirmé que la directive ne mettait pas en place les protections nécessaires des droits fondamentaux, tout en n'écartant pas la possibilité que les États membres, individuellement, usent de leur marge de manœuvre à cette fin.[347]

344 Conseil de l'Europe, Economic Crime Division of the Directorate General of Human Rights and Legal Affairs, *Project on Cybercrime Final report (septembre 2006-février 2009)*, ECD/567(2009)1, Strasbourg, 15 juin 2009, 51 pp. [en ligne] (consulté le 20 août 2015) http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy%20Project/567-d-final%20report1i%20final%20_15%20june%2009_.pdf et *Global Project on Cybercrime (Phase 2) 1 March 2009 – 31 December 2011 Final project report*, Strasbourg, 9 avril 2012, 43 pp. [en ligne] (consulté le 20 août 2015) http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079_adm_finalreport_V12_9apr12.pdf.

345 Voir lexique, entrée **Fournisseur de services Internet**.

346 Directive 2006/24/CE du Parlement européen et du Conseil, du 15 mars 2006, sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la directive 2002/58/CE (JO L 105, p. 54).

347 CEDH, Requête n°2872/02, 2 décembre 2008, *K.U. c/ Finlande*.

En 2014, la CJUE l'a finalement invalidée, estimant qu'elle créait une ingérence d'une vaste ampleur et d'une gravité particulière dans les droits fondamentaux au respect de la vie privée et à la protection des données à caractère personnel sans être pour autant limitée au strict nécessaire. Elle aurait dû prévoir une information de l'abonné ou de l'utilisateur inscrit, introduire une différenciation entre les individus et les catégories de données. Pour être conforme au droit international, ici de l'UE, elle devrait encadrer l'accès aux données par les autorités compétentes de façon à éviter les abus et elle n'assure pas une protection et une sécurité suffisantes.[348]

La préservation de l'ordre public dans la plupart des ordres juridiques nationaux signifie que les décisions de justice étrangères ne peuvent être exécutées que si elles sont conformes à un corpus de principes fondamentaux, tant nationaux qu'issus du droit international.[349] Le niveau de protection garanti à l'échelle nationale par nos partenaires internationaux devra donc être pris en compte dans notre action en matière de lutte contre le trafic de données personnelles en ligne. Aujourd'hui, la plupart des États reconnaissent une certaine liberté d'expression en ligne.[350]

Aux États-Unis, en particulier, la liberté d'expression, garantie par le Premier Amendement à la Constitution, est farouchement défendue dans le cadre d'Internet,[351] où elle implique un véritable droit à l'anonymat,[352] certains aménagements restant envisageables pour protéger le droit d'auteur, notamment.[353]

La question de la responsabilité des FSI échappe majoritairement à la compétence fédérale, certains États comme le Mississippi lui étant plus favorables que des paradis de la dérégulation en ligne, comme le Maine ou la Californie.[354]

348 CJUE, Affaires jointes C-293/12 et C-594/12, 8 avril 2014, *Digital Rights Ireland et Seitlinger e.a.* déjà citée.
349 Dans le cadre du droit international privé, c'est l'exception d'ordre public qui conditionnera par exemple l'exequatur: Parlement Européen, Direction générale des politiques internes, Affaires juridiques et parlementaires, 2011, *Interprétation de l'exception d'ordre public telle que prévue par les instruments du droit international privé et du droit procédural de l'Union*, Étude PE 453.189, 181 pp. [en ligne] (consulté le 20 août 2015) http://www.europarl.europa.eu/RegData/etudes/etudes/join/2011/453189/IPOL-JURI_ET(2011)453189_FR.pdf.
350 Les juridictions indiennes, par exemple, ont pu invalider des projets de l'Exécutif, vue la limitation grave qu'ils auraient imposée à la liberté d'expression : Amnesty International, *India: Historic Supreme Court ruling upholds online freedom of expression*, 24 mars 2015 [en ligne] (consulté le 20 août 2015) https://www.amnesty.org/en/latest/news/2015/03/india-supreme-court-upholds-online-freedom-of-expression/.
351 SHELL Meredith, *Network Neutrality and Broadband Service Providers' First Amendment Right to Free Speech*, Federal Communications Law Journal, Volume 66, pp. 303-326 [en ligne] (consulté le 20 août 2015) http://www.fclj.org/wp-content/uploads/2014/06/66.2.3_Shell-Final.pdf.
352 États-Unis, Supreme Court, n°93-986, 19 avril 1995, *McIntyre v. Ohio Elections Comm'n* [en ligne] (consulté le 20 août 2015) http://caselaw.findlaw.com/us-supreme-court/514/334.html.
353 États-Unis, District Court for the district of Columbia, Civil Action n°11-1741 (JDB/JMF), *Hard Drive Productions, Inc. v/ Does*, 26 septembre 2012 [en ligne] (consulté le 20 août 2015) http://law.justia.com/cases/federal/district-courts/district-of-columbia/dcdce/1:2011cv01741/150362/54/.
354 BHANDARI Esha, BRENNAN FELLOW William, HOSSAIN Samia, *Mississippi's All Up in Your Google Activity*, American Civil Liberties Union (ACLU), 3 août 2015 [en ligne] (consulté le 20 août 2015) https://www.aclu.org/blog/speak-freely/mississippis-all-your-google-activity et ACLU, *Communications Decency Act Section 230* [en ligne] (consulté le 20 août 2015) https://www.aclu.org/issues/free-speech/internet-speech/communications-decency-act-section-230.

Une solution possible à la méfiance réciproque des États est le dialogue au sein de forums ou d'organisations internationaux. Un tel organisme, le Groupe d'Action Financière sur le Blanchiment de Capitaux (GAFI) a été créé par lors du Sommet du G7 qui s'est tenu à Paris en juillet 1989. Sa mission était d'examiner et d'élaborer des mesures de lutte contre le blanchiment de capitaux. Ses objectifs ont été de nouveau fixés en avril 2012, ils comprennent l'élaboration des normes et la promotion de l'efficace application de mesures législatives, réglementaires et opérationnelles en matière de lutte contre le blanchiment de capitaux, le financement du terrorisme et les autres menaces liées pour l'intégrité du système financier international.

La Commission européenne est l'un des 36 membres du GAFI et s'intéresse beaucoup à ses travaux. Le Groupe s'est efforcé de développer une stratégie permettant d'adapter les investigations financières aux particularités de la lutte contre le trafic de données personnelles.

Titre II : Une adaptation des outils de l'investigation financière

Un autre moyen, pour l'Union européenne, de faciliter la lutte contre la cybercriminalité tiendrait à la mise en œuvre et à l'adaptation des outils de l'investigation financière contre les cybercriminels. Il y a une volonté globale de se livrer à une investigation financière des trafiquants de données personnelles (**Chapitre 1**) mais les enquêteurs financiers doivent s'adapter à la réalité du *cybercrime-as-a-service* (**Chapitre 2**).

Chapitre 1 : La volonté de se livrer à des investigations financières des activités cybercriminelles

Il existe aujourd'hui une vraie volonté de systématiser le recours à l'investigation financière dans tous les domaines de la criminalité organisée, dont le trafic de données personnelles (*section 1*). Il s'agit d'une méthode prometteuse, qui pourrait permettre la saisie des avoirs criminels issus de ce trafic (*section 2*) mais aussi peut-être l'identification des trafiquants de données personnelles (*section 3*).

Section 1 : La systématisation du recours à l'investigation financière

Il peut sembler curieux de parler d'« investigation financière » alors que cette enquête apparaît tardivement au stade de la recherche de l'infraction ou de son auteur. En effet, si l'investigation financière a fait son apparition dans le domaine de la criminalité organisée, c'était d'abord à des fins de gel et de saisie des avoirs. Ceux-ci jouent un rôle dissuasif et font obstacle à la reprise ultérieure des activités criminelles après une première condamnation. L'investigation financière a ensuite révélé son intérêt en termes d'établissement de la preuve pénale, particulièrement dans le cas des infractions financières.

L'actuelle promotion de l'utilisation systématique de l'investigation financière dans les enquêtes en matière de criminalité organisée viserait plutôt le recouvrement des avoirs d'origine criminelle,[355] exception faite de la lutte contre la traite des êtres humains.

355 PETIT Bernard, *Une nouvelle approche de la lutte contre la criminalité organisée : la prise en compte du volet financier des enquêtes*, AJ Pénal, 2012, p. 148.

L'UE s'est efforcée de développer une véritable réflexion, alimentée par la perspective d'une nouvelle modalité de recherche de preuve. Dans sa stratégie en vue de l'éradication de la traite des êtres humains de 2012, la Commission recommande de mener activement des investigations financières afin d'épargner aux victimes la peine de devoir témoigner. Elle suggère également qu'il serait possible de détecter les infractions par ce biais et charge Europol de rédiger un rapport sur les bonnes pratiques et les avantages de l'investigation financière.[356]

L'agence s'y est efforcée au cours de l'année passée, s'employant à analyser le modèle économique des groupes criminels, l'objet et le bénéfice des investigations financières, le cadre judiciaire, les techniques d'enquête et aussi l'approche multidisciplinaire à adopter.[357]

Ce travail semble confirmer ce que craignaient les experts : l'investigation financière apparaît très prometteuse mais ne peut réussir que si elle intervient dans le cadre d'enquêtes intégrées et pluridisciplinaires. La plus grande difficulté est d'amener les forces de l'ordre à coopérer avec des unités de renseignement financier dont la nature est souvent encore purement administrative.[358]

Néanmoins, une telle approche multidisciplinaire apparaît prometteuse.

Section 2 : Le gel et la confiscation des avoirs criminels issus du trafic de données personnelles grâce à l'investigation financière

Le recours systématique à l'investigation financière pourrait permettre le gel et la confiscation des profits que génère le trafic de données personnelles. L'UE encourage ceux-ci au

356 « *Conformément aux recommandations du Groupe d'action financière de l'Organisation de coopération et de développement économique,* ***les États membres doivent*** *en 2013* ***mener activement des investigations financières dans les affaires de traite des êtres humains****, fournir des informations pour le fichier de travail à des fins d'analyse d'Europol et renforcer leur coopération avec les agences de l'UE, telles qu'Eurojust et le Collège européen de police (CEPOL).* ***Europol procédera*** *d'ici 2015* ***à une analyse des informations transmises par les États membres sur les investigations financières dans les affaires de traite des êtres humains****. Cette analyse devrait permettre de dégager de bonnes pratiques ainsi que des modèles pour les enquêtes policières financières. L'investigation financière est un outil reconnu pour recueillir des éléments de preuve. Dans de nombreuses enquêtes sur des affaires de traite d'êtres humains, la collecte des éléments de preuve en vue de poursuivre les trafiquants repose encore en grande partie sur le témoignage des victimes. Les indices fournis par les pistes financières, en particulier dans les secteurs à hauts risques, pourraient fournir les preuves supplémentaires requises et épargner ainsi aux victimes l'épreuve d'un témoignage à la barre. Les investigations financières pourraient également jouer un rôle utile dans l'évaluation des risques et aider à mieux connaître le mode opératoire des auteurs d'infractions liées à la traite des êtres humains et à affiner les outils de détection.* », Commission Européenne, Bruxelles, 19 juin 2012, Communication COM(2012) 286 final, *La stratégie de l'UE en vue de l'éradication de la traite des êtres humains pour la période 2012-2016*, p. 11 [en ligne] (consulté le 20 août 2015) http://ec.europa.eu/home-affairs/doc_centre/crime/docs/trafficking_in_human_beings_eradication-2012_2016_fr.pdf.

357 Portail Europe liberté sécurité et justice, *Le Trafic et la Traite des êtres humains : désorganiser la criminalité transfrontalière organisée*, 6 mai 2015 [en ligne] (consulté le 20 août 2015) http://europe-liberte-securite-justice.org/2015/05/06/le-trafic-et-la-traite-des-etres-humains-desorganiser-la-criminalite-transfrontaliere-organises/.

358 DUMOULIN Lisa, *Lutte contre la traite des êtres humains : l'approche financière en question*, RSC, 2014, p. 311.

moins depuis la décision-cadre du 26 juin 2001 concernant le blanchiment d'argent, l'identification, le dépistage, le gel et la confiscation des instruments et des produits du crime, qui imposait surtout le respect des obligations conventionnelles qu'ils avaient contractées dans le cadre du Conseil de l'Europe.

La législation de l'UE en matière d'identification a ensuite été améliorée par le biais de la coopération intergouvernementale, avec la création de bureaux de recouvrement des avoirs (ARO) dans les États, qui collaboreraient entre eux. En France, par exemple, sont reconnus comme des ARO depuis 2007 la Plateforme d'Identification des Avoirs Criminels (PIAC), composée de policiers et de gendarmes, et rattachée à l'Office Central pour la Répression de la Grande Délinquance Financière (OCRGDF) du Ministère de l'Intérieur et l'Agence de Gestion et de Recouvrement des Avoirs Saisis et Confisqués (AGRASC). Par ailleurs, à l'échelle internationale, la France participe au réseau CARIN (*Camden Asset Recovery Inter-agency Network*) qui regroupe les ARO, l'« *Egmont Group of Financial Intelligence Units* », groupement informel d'unités d'intelligence financière qui recueille et sélectionne les informations sur les activités financières suspectes et à l'initiative STAR (*Stolen Asset Recovery*) de la Banque mondiale et de l'Office des Nations Unies contre la drogue et le crime (ONUDC).

Quant à la saisie, un mécanisme basé sur la reconnaissance mutuelle a été adopté par la décision-cadre 2003/577/JAI. Puis, une harmonisation s'avérant nécessaire, la directive 2014/42/UE a été adoptée.

Dans un rapport de 2011 sur l'identification des avoirs, la Commission s'estimait globalement satisfaite et optimiste quant aux ARO et à leur réseau : ses chiffres semblaient indiquer que ces organes fonctionnaient bien et collaboraient de plus en plus.[359] Il n'y a pas de raisons d'imaginer que les biens des trafiquants de données personnelles soient d'une nature leur permettant d'échapper à l'identification, au gel et à la confiscation. En effet, s'ils manifestent une certaine opacité, elle n'est que transitoire. La capacité même d'instruments comme les monnaies virtuelles à assurer l'intraçabilité des fonds les rend relativement instables et en fait donc de piètres valeurs de capitalisation, limitant leur intérêt aux seuls échanges.

Il en va de même de l'usurpation d'identité, qui peut participer à la dissimulation des fonds mais qui ne se prête pas non plus à la conservation des biens, du fait du risque continu de découverte.

359 Commission Européenne, *Rapport fondé sur l'article 8 de la décision 2007/845/JAI du Conseil du 6 décembre 2007 relative à la coopération entre les bureaux de recouvrement des avoirs des États membres en matière de dépistage et d'identification des produits du crime ou des autres biens en rapport avec le crime*, Communication COM(2011) 176 final, 12 avril 2011.

Section 3 : L'identification des trafiquants de données personnelles par l'investigation financière

L'utilisation d'identités usurpées comme le recours au *smurfer* et les autres moyens du blanchiment peuvent être détectés et révéler l'infraction cybercriminelle sous-jacente. Tout comme l'enquêteur est proactif sur Internet, il lui faut aussi dans le champ de l'investigation financière aller au-devant du trafic de données personnelles sans attendre que l'activité lui soit révélée.

Deux types d'indices peuvent le guider dans son action. Le premier tient aux moyens du blanchiment. Suivant leurs conditions d'utilisation, les moyens de paiement seront plus ou moins attractifs pour les criminels et l'étude de ces caractéristiques peut permettre d'évaluer ce que l'on appellera « le risque » de tel ou tel instrument et sur lequel on reviendra dans une partie ultérieure.

Le second type d'indices ne tient pas aux moyens car le blanchiment s'effectuera par le biais d'opérations tout à fait anodines, mais à l'identité de l'opérateur. En effet, dans le cas des trafiquants de données personnelles tout particulièrement, l'usurpation d'identité aux fins de blanchiment doit être monnaie courante. Il faut alors surveiller, bien sûr, les éventuelles incohérences dans les informations sur l'utilisateur, le volume des comptes et de leurs transactions, les transactions répétitives et/ou massives vers/depuis d'autres comptes, la liquidation massive des fonds, l'absence de dépenses, hors retrait, etc.[360]

Les questions de l'usurpation d'identité et des nouveaux moyens de paiement contraignent néanmoins l'enquêteur financière à rénover son approche.

360 Organisation de Coopération et de Développement Économiques (OCDE), *Rapport sur l'usurpation d'identité et la fraude à l'identité : risques lies a la fraude fiscale et au blanchiment de capitaux centre de politique et de l'administration fiscales*, 25 février 2009, 20 pp..

Chapitre 2 : L'évolution de l'enquêteur financier face au cybercrime comme service de blanchiment d'argent

L'enquêteur financier doit s'adapter à des criminels susceptibles d'usurper des identité pour blanchir leurs gains illicites (*section 1*) et de réaliser leurs échanges et leur blanchiment via de nouvelles méthodes de paiement (*section 2*). Il lui faut pour cela développer une expertise informatique, en plus de l'expertise financière (*section 3*).

Section 1 : L'adaptation de l'investigation financière à l'usurpation d'identité

Dès 2013, dans une résolution, le Parlement Européen remarquait les relations croissantes entre organisations criminelles et la maximisation des profits par le biais de la spécialisation, ce que nous avons évoqué brièvement sous l'étiquette « *Cybercrime-as-a-service* »[361]

Les trafiquants de données personnelles utilisent mais aussi pourvoient à d'autres formes de criminalité, comme le blanchiment d'argent. Alors qu'au début des années 2000, la fraude à l'identité et l'usurpation d'identité étaient principalement associées à des types de fraudes mineures,[362] dès avant les années 2010, la plupart des États signalaient l'utilisation d'identités usurpées pour blanchir des capitaux et, parmi les procédés les plus courants, la création d'une fausse identité à partir de données volées et son utilisation frauduleuse pour créer une entreprise, ouvrir un compte bancaire, imprimer des fausses factures, etc, afin de générer de faux profits dissimulant les gains illégaux.[363]

Les autorités avaient déjà développé un certain nombre de stratégies et techniques de détection : la collecte de renseignements, l'analyse du risque, l'établissement de profils de risque et le recoupement systématique des données pour repérer les éventuels cas de blanchiment de capitaux avec usurpation d'identité.

La plupart des pays fait intervenir l'administration fiscale, les banques et les autorités des marchés financiers, ainsi que d'autres professionnels (avocats, notaires, etc, bien connus pour leur implication dans les activités anti-blanchiment). Au Canada, on a signalé rapidement le recours à

361 Parlement Européen, *La criminalité organisée, la corruption et le blanchiment de capitaux: recommandations sur des actions et des initiatives à entreprendre (rapport à mi-parcours)* (2012/2117(INI)), Résolution P7_TA(2013)0245 A7-0175/2013, Strasbourg, 11 juin 2013.
362 Canada, Groupe de travail binational sur les fraudes transfrontalières par marketing de masse, *Rapport sur le vol d'identité*, Rapport présenté à la ministre de la Sécurité publique et de la Protection civile du Canada et à l'Attorney General des États-Unis, octobre 2004 [en ligne] (consulté le 20 août 2015) http://www.securitepublique.gc.ca/cnt/rsrcs/pblctns/archive-dntt-thft-rprt/index-fra.aspx#a09.
363 OCDE, op. cit.., p. 12.

des équipes spécialisées dans les cas d'usurpation d'identité au sein des investigations financières. Cette stratégie apparaît plus efficace que le rattachement du Bureau de programme chargé des questions d'usurpation d'identité à l'administration fiscale (IRS) aux États-Unis.

C'est également au Canada que l'utilisation d'outils informatiques de croisement automatique des données (à la recherche de dédoublement, etc) a été précocement expérimentée. Au Royaume-Uni, plutôt que par la systématisation des recoupements, la détection d'éventuelles irrégularités est effectuée par des programmes d'interrogation aléatoires pour déceler d'éventuelles irrégularités, avec une certaine concentration en fonction du risque, ce qui paraît moins attentatoire au droit à la vie privée. La Suède règle le problème de façon radicale : elle propose un modèle de transparence complète. Tout citoyen pouvant vérifier le contenu des différents registres le mentionnant, il peut immédiatement les corriger ou signaler une incohérence. Une application stricte des principes de traitement des données personnelles, ici le droit d'accès, permet donc, dans une certaine mesure, de lutter contre l'utilisation frauduleuse de données personnelles à l'échelle de chaque individu.[364]

À côté de cet abus des données personnelles au sein de mécanismes classiques de blanchiment d'argent, les trafiquants de données personnelles peuvent aussi faire usage des nouveaux moyens de paiement. L'UE s'est alignée sur le GAFI et a adopté l'approche par les risques pour lutter contre ces méthodes de blanchiment.

Section 2 : L'approche par les risques du blanchiment d'argent via les nouvelles méthodes de paiement

Les nouveaux instruments de paiement font partie de l'offre de *Cybercrime-as-a-service* dont profitent les criminels traditionnels. Ils sont donc entrés assez rapidement parmi les centres d'intérêts des enquêteurs financiers. Le GAFI, un organisme intergouvernemental créé en 1989 et faisant la promotion de l'investigation financière, a conseillé dès 2006 aux autorités de ses États membres d'adopter, face aux nouveaux instruments de paiement, une approche par le risque.[365]

Bien avant de reconnaître que les nouvelles méthodes de paiement ne servaient pas que des projets illégitimes et n'offraient pas toutes un terrain également fertile aux criminels souhaitant blanchir leur argent,[366] le GAFI était favorable à un système déclarationnel responsabilisant les fournisseurs

364 Ibid, pp. 11-12.
365 Groupe d'Action FInancière (GAFI), *New Payment Methods*, Rapport, 13 octobre 2006, 40 pp..
366 « *NPMs have developed as a result of the legitimate need of the market for alternatives to traditional financial services.* », GAFI, *Money Laundering Using New Payment Methods*, Rapport, octobre 2010, p. 12.

de services financiers. Les professionnels ont la charge de déterminer quel niveau de vigilance imposer à leur clientèle dans l'exercice de leurs activités suivant un risque de blanchiment qu'il leur appartient de définir.

Celui-ci se décline en fait en deux volets. D'une part, la clientèle implique un niveau de vigilance variable. D'autre part, certaines transactions présente un risque accru.

Naturellement, dans le cas des nouvelles méthodes de paiement, particulièrement propices à l'anonymat, ces deux catégories se fondent en une seule, qui tient davantage à la nature du produit fourni. En 2010, dans un second rapport, le GAFI a donc précisé les critères pour évaluer le risque présenté par chaque nouvel instrument de paiement.

Il notait d'abord que les criminels sont en quête de moyens de paiement satisfaisant leurs exigences d'anonymat, de volumes et d'accessibilité des fonds. Or, les nouvelles méthodes de paiement (NMP) génèrent des risques du fait de leur nature prépayée (les sociétés ne prennent aucun risque en termes de crédit), de la rapidité des transactions et de l'absence de relations commerciales en face-à-face. Elles auraient facilité le blanchiment selon trois méthodes particulières : l'utilisation de fonds de tiers (hommes de pailles, *smurfers*, etc), l'exploitation de l'absence de face-à-face, ainsi que la complicité des fournisseurs de nouveaux services de paiement et de leurs employés.

La matrice des risques inclut quatre critères : l'identification (identification des clients, vérification de leur identité et surveillance des points de vente et sous-traitants), la tenue des registres, la limitation de l'usage, de la valeur et la segmentation des services. Le tableau en annexe 50 résume ces critères.[367] Pour bien lire cette matrice, il faut noter que le fait, pour une monnaie d'être à haut risque selon une catégorie ne signifie pas nécessairement qu'elle devra suivre les obligations qui accompagnent la qualification de NMP à haut risque.

PayPal, par exemple, est une NMP à haut risque du point de vue des limites géographiques mais, comme on l'a vu, les cyberdélinquants la dédaignent en raison de la limitation de la valeur (bas risque).

Le pack anti-blanchiment d'argent de 2015 se réfère expressément aux lignes directrices du GAFI et à l'approche par le risque.[368] Son avantage est qu'elle est extensible et peut admettre de

367 Voir **Annexe 50 : Matrice des risques des nouvelles méthodes de paiements**.

368 *Règlement (UE) 2015/847*, paragraphe 23 : « *Conformément à l'approche fondée sur les risques mise au point par le GAFI, il convient d'identifier les domaines où les risques sont plus élevés et ceux où ils sont plus faibles, de manière à mieux cibler les risques de blanchiment de capitaux et de financement du terrorisme.* » Une telle référence explicite n'est pas nouvelle. Déjà, par exemple, au considérant 5 de sa directive 2005/60/CE du 26 octobre 2005 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux et du financement du terrorisme, l'Union européenne expliquait que « *le blanchiment de capitaux et le financement du terrorisme s'inscrivent souvent dans un contexte international. Des mesures adoptées au seul niveau national ou même communautaire, sans coordination ni coopération internationales, auraient donc des effets très limités. Par conséquent, les mesures arrêtées*

nouveaux critères et de nouvelles monnaies. Elle va cependant aussi présenter aux législateurs un dilemme. En effet, elle suppose une appréciation relative, celle des risques, et les seuils dégagés pour réaliser cette évaluation seront plus ou moins englobants : un seuil élevé permettra l'inclusion de davantage de NPM parmi celles soumises à une surveillance accrue, générant un coût financier et humain pour les autorités, ainsi qu'un risque de faire fuir les utilisateurs légitimes vers des moyens de paiement moins bien connus, réguliers et fiables, un seuil bas pourrait rendre la surveillance des autorités complètement dénuée d'effets.

Dans un contexte de gestion managériale des ressources de la Justice et de la Police, l'enjeu d'élever au maximum le seuil du risque se posera en des termes de plus en plus pressants. L'interlocuteur français du GAFI, la cellule de Traitement du Renseignement et Action contre les Circuits FINanciers clandestins (TRACFIN), remplit l'essentiel des exigences de celui-ci, un certain manque de moyens excepté. La Cour des Comptes le signalait en 2012[369] et les chiffres de 2014 ne traduisent pas d'amélioration majeure des capacités de traitement de TRACFIN.[370]

Néanmoins, la Cour soulignait que le niveau de déclaration des professions assujetties n'était pas égal et qu'il y avait certainement là une lacune du système déclaratif.[371] On ne peut que se demander si cette faille n'est pas plus critique encore dans le cadre de l'approche par les risques des nouveaux moyens de paiement. Quel est l'intérêt de ces intermédiaires, recherchés pour leur opacité, à faire preuve de transparence avec les forces de l'ordre ?

Peut-être serait-il souhaitable que le GAFI envisage un dispositif pour s'assurer que les déclarations soient fidèles à la réalité.

À côté des nouveaux moyens de paiement, le blanchiment d'argent a été facilité par l'apparition de nouvelles places d'échange en ligne, qui semblent nécessiter une nouvelle formation et de nouveaux partenariats pour l'enquêteur financier.

par la Communauté en la matière devraient être compatibles avec toute autre action engagée dans d'autres enceintes internationales. En particulier, la Communauté devrait continuer à tenir compte des recommandations du Groupe d'action financière internationale (dénommé ci-après «GAFI»), qui est le principal organisme international de lutte contre le blanchiment de capitaux et contre le financement du terrorisme. Les recommandations du GAFI ayant été largement modifiées et développées en 2003, la présente directive devrait être en harmonie avec les nouvelles normes internationales. »

369 Cour des comptes français, *TRACFIN et la lutte contre le blanchiment d'argent*, Rapport public annuel 2012, février 2012, pp. 197-228.

370 Ministère des Finances et des Comptes Publics, Traitement du Renseignement et Action contre les Circuits FINanciers clandestins (TRACFIN), *Rapport annuel d'activité tracfin 2014*, 2015, 62 pp. : en 2012, la Cour des comptes signalaient la lenteur de l'augmentation du nombre de transmissions judiciaires malgré la multiplication des signalements reçus par TRACFIN. Elle situait alors le nombre de transmissions aux alentours de 400. En 2014, il y en a eu 464, soit une augmentation de 1,5 % seulement, par rapport à 2013.

371 Cour des comptes, Op.cit., pp. 203-204.

Section 3 : La mise en commun des compétences avec le secteur de l'informatique

Comme nous l'avons vu au sujet des MMORPG, il existe de véritables tronçons d'économie parallèle sur Internet, facilitant le blanchiment d'argent. Ils offrent un moyen presque infaillible de disperser et transférer les produits provenant d'activités de criminalité organisée. Par exemple sur le jeu *World of Warcraft* (WOW), les criminels achètent des pièces d'or virtuelles à des complices. Ensuite, l'argent est dispersé, les criminels ouvrant des centaines de comptes distincts, mettant en place des mécanismes d'échanges complexes entre ceux-ci, puis réunissant les pièces d'or blanchies sur un compte unique, dont le contenu sera vendu légitimement à un autre utilisateur, contre de l'argent réel.

Les problèmes juridictionnels que posent ces MMORPG pourraient aisément être contournés si les entreprises qui créent et administrent des mondes virtuels se faisaient le relais de l'action des États mais ces compagnies, déjà peu désireuses de prêter le flanc aux critiques, ne souhaitent pas être soumises par les autorités à des obligations de traitement plus dures. Il est vrai qu'elles manifestent une réelle volonté de détecter ces pratiques illicites. Alors que leur expertise informatique leur permet de détecter certains mouvements de fonds douteux, néanmoins, il leur manque l'expertise de véritables enquêteurs financiers.[372]

Le même raisonnement s'applique aux *alt-coins*. Bien que l'émission de ces fonds soit décentralisée, leur création par minage place un certain nombre d'entreprises au centre du réseau. Il faudrait les encourager à pratiquer la revente des devises minées d'une façon plus éthique et contrôlable – peut-être par leur intégration au nombre des opérateurs tributaires de l'approche par le risque, au même titre que les autres NMP. Le marché des *crypto-monnaies* ne se réduit pas après tout aux seuls criminels soucieux de blanchir leurs gains illicites.

Alors que les opérateurs privés ont une expertise informatique à offrir, en plus de leur capacité à contrôler l'univers virtuel qu'ils sous-tendent, au contraire des partenaires sur lesquels l'enquêteur financier devait auparavant se reposer, il leur manque bien souvent une expertise financière et de lutte contre le blanchiment d'argent.

Celle-ci peut parfois leur causer un préjudice – direct dans le cas des dommages subis par les utilisateurs et que la société gestionnaire répare généralement, ou dû à la perte de revenus et aux conséquences des incidents pour sa réputation. L'exemple des chaînes de Ponzi est significatif à ce

372 Centre d'analyse des opérations et déclarations financières du Canada (CANAFE), *Regard sur le blanchiment d'argent et le financement des activités terroristes*, octobre à décembre 2010, pp. 6-7 [en ligne] (consulté le 20 août 2015) http://publications.gc.ca/collections/collection_2011/canafe-fintrac/FD3-1-8-2010-fra.pdf.

titre.

Le recours systématique à l'investigation financière dans les cas de trafic de données personnelles apparaît prometteur pour l'identification, le gel et la confiscation des avoirs criminels, l'établissement de la preuve des infractions mais aussi la recherche des infractions et de leurs auteurs. L'UE fournit des outils intéressants de promotion de l'investigation financière. L'intégration de l'enquêteur financier et des forces de police n'est cependant pas encore assez complète, notamment dans le cas de l'usurpation financière à des fins de blanchiment. Il faut également perfectionner l'approche par les risques et l'étendre à tous les opérateurs intervenant dans le blanchiment d'argent en ligne. L'UE s'est aussi dotée d'une expertise analytique et opérationnelle, ainsi que d'outils procéduraux de coopération opérationnelle entre forces de police, autorités judiciaires nationales et agences de l'UE, tant à l'international que dans l'Union. Les législations sur les données personnelles doivent être étendues pour traiter du volet pénal et celles sur la cybercriminalité se heurtent à des réticences de ses homologues nationaux.

Conclusion

Le législateur de l'UE a donc offert une réponse aux lacunes de la définition des données personnelles, de la cybercriminalité et des trafiquants de données sur Internet mais les législateurs des États membres ont insuffisamment transposé ces dispositions. L'Union s'efforce d'établir une responsabilité des opérateurs Internet permettant l'exécution des décisions de justice. Elle a également créé de nouveaux moyens d'investigation, de coopération et de coordination, comme l'équipe commune d'enquête, Europol et le mandat d'arrêt européen, qu'elle essaie d'étendre peu à peu aux États tiers.

L'Union encourage aussi la naissance d'un nouveau type d'enquêteur, proactif, apte à recueillir des preuves pénales dans le monde électronique. Le trafic de données personnelles impliquant essentiellement le crime organisé, l'UE est favorable au recours systématique à l'investigation financière dans ce domaine, à des fins de gel et de confiscation des avoirs criminels, de preuve ou d'identification des trafiquants. L'enquêteur financier européen a développé une expertise informatique, s'est adapté à l'utilisation de l'usurpation d'identité pour le blanchiment et a élaboré une approche par les risques des nouvelles méthodes de paiement.

Il est crucial que les législateurs, les enquêteurs et les autorités judiciaires suivent son exemple. Le trafic de données personnelles peut passer pour une activité criminelle de peu d'importance : ses victimes ne sont pas atteintes dans leur intégrité physique et les dommages engendrés sont essentiellement d'ordre financier ou tiennent de la simple perte de temps et d'énergie. Il ne faut pas le sous-estimer pour autant.

L'offre de la cyberdélinquance comme service signifie qu'elle facilite de nombreuses autres formes de criminalité. Le terrorisme compte au nombre de celles-ci. Dès 2013, le Parlement Européen soulignait la coopération entre les organisations criminelles (les cartels sud-américains et le crime organisé russophone).[373] Les organisations terroristes ont d'énormes fonds, qu'elles ont besoin de mobiliser sur des territoires où leurs activités sont complètement illégales.[374] Dès 2005, dans le cadre de la lutte contre le terrorisme, l'UE préconisait de priver les terroristes des moyens de leur action (faux documents, moyens de communication clandestins, moyens d'échanges financiers, etc). Cela passe aussi par le démantèlement des réseaux de trafic de données personnelles.[375]

373 Parlement Européen, *La criminalité organisée, la corruption et le blanchiment de capitaux : recommandations sur des actions et des initiatives à entreprendre (rapport à mi-parcours)* (2012/2117(INI), Résolution P7_TA(2013)0245 A7-0175/2013, Strasbourg, 11 juin 2013.
374 MASCRÉ Celia, *Trois femmes tchétchènes arnaquent Daech en beauté*, Geopolis, 31 juillet 2015 (en ligne) [consulté le 20 août 2015] http://geopolis.francetvinfo.fr/trois-femmes-tchetchenes-arnaquent-daech-en-beaute-73199.
375 Conseil de l'Union européenne, *Stratégie de l'Union européenne visant à lutter contre le terrorisme*, Bruxelles, 30

Bibliographie

OUVRAGES

VIDOCQ, *Mémoires de Vidocq*, Chef de la police de sûreté jusqu'en 1827, Tome 1, Ebooks libres, 1828, 255 pp..

MITNICK Kevin, SIMON William, *The art of deception - Controlling the Human Element of Security*, Wiley Publishing Inc., Indianapolis, Indiana, États-Unis, 2002, 352 pp..

MITNICK Kevin, SIMON William, *The art of intrusion - The Real Stories Behind the Exploits of Hackers, Intruders & Deceivers*, Wiley Publishing Inc., Indianapolis, Indiana, États-Unis, 2005, 270 pp..

LEFEBURE Antoine, *L'affaire Snowden. Comment les États-Unis espionnent le monde*, La Découverte, Paris, février 2014, 275 pp..

KREBS Brian, *Spam nation : the inside story of organized cybercrime—from global epidemic to your front door*, Sourcebooks Inc, Naperville, Illinois, États-Unis, 18 novembre 2014, 256 pp..

TRAVAUX UNIVERSITAIRES

HAUT François (dir.), *Les gangs de motards criminalisés*, Mémoire de l'Institut de Criminologie de Paris, Département de recherche sur les Menaces Criminelles Contemporaines (Université de Paris II Panthéon-Assas), août 2001, 160 pp..

ROCHEFORT-MARANDA Catherine, *Analyse de la position des groupes et des individus dans un réseau criminel structuré autour des motards criminalisés*, Mémoire de l'École de Criminologie, Université de Montréal, août 2010, 159 pp. [en ligne] (consulté le 11 septembre 2015) https://papyrus.bib.umontreal.ca/xmlui/bitstream/handle/1866/4908/Rochefort-Maranda_Catherine_CRM_2011_memoire.pdf;jsessionid=546E02EA0C431B73877F76C17AE2E26F?sequence=2.

MATIGNON Emmanuelle, *La cybercriminalité: Un focus dans le monde des télécoms*, Mémoire Master Droit du numérique Administrations - Entreprises de l'École de droit de la Sorbonne (Université Paris 1 Panthéon-Sorbonne), année universitaire 2011/2012, 95 pp..

CHRISTIN Nicolas, *Traveling the Silk Road: A measurement analysis of a large anonymous online*

novembre 2005, 14469/3/05 REV 3 JAI 423 ECOFIN 353 TRANS 234 RELEX 639 ECO 136 PESC 1010 COTER 72 COSDP 810 PROCIV 174 ENER 172 ATO 103, paragraphes 28 et 29.

marketplace, « *Customer satisfaction* », Université Carnegie Mellon, College of Engineering's cybersecurity laboratory (CyLab), Pittsburgh, Pennsylvanie, États-Unis, 1er août 2012, 24 pp..

PAPACOSTAS Melina, *Projet de réforme européenne sur la protection des données personnelles, enjeux français et anglais*, Université Paris Ouest Nanterre La Défense - Société de l'information, droits et médias, 21 avril 2013 [en ligne] (page consulté le 20 août 2015) http://m2bde.u-paris10.fr/node/2515?destination=node%2F2515.

FLOREAN Alejandro, GANTZ John, KUMAR SRISTI LAKSHMI Sravana, LEE Richard, LIM Victor, MADHAVAN Logesh, NAGAPPAN Mangalam et SIKDAR Biplab, *The Link between Pirated Software and Cybersecurity Breaches How Malware in Pirated Software Is Costing the World Billions*, Université Nationale de Singapour et International Data Corporation (IDC), Étude conjointe IDC #247411, mars 2014, 35 pp..

ARTICLES

- **Doctrine Française**

PADOVA Yann, *Un aperçu de la lutte contre la cybercriminalité en France*, RSC, 2002, p. 765.

BÉNICHOU David, *Cybercriminalité : jouer d'un nouvel espace sans frontière*, AJ Pénal, 2005, p. 224.

FÉRAL-SCHUHL Christiane, *Une procédure pénale adaptée à l'internet se dessine : entre « cyber-enquêteurs » et collaboration des fournisseurs et utilisateurs*, AJ Pénal, 2005, p. 228.

MASOUNAVE Annick, *Enquête Le système financier de Second Life*, Revue Banque, hors-série « Second Life », octobre 2007, pp. 11-16.

FILIOL Éric, *Notes sur les méthodes techniques d'acquisition de la preuve Virus et vers « enquêteurs »*, Séminaire « Criminalité en Europe », Laboratoire de virologie et de cryptologie, École Supérieure et d'Application des Transmissions (ESAT), 5 juillet 2007, 14 pp..

HALPÉRIN Jean-Louis, *La preuve judiciaire et la liberté du juge*, Communications, Numéro 84, « Figures de la preuve », 2009, pp. 21-32 [en ligne] (consulté le 20 août 2015) http://www.persee.fr/web/revues/home/prescript/article/comm_0588-8018_2008_num_84_1_2504.

FALLERY Bernard et RODHAIN Florence, *Fondements théoriques pour une régulation d'Internet : La légitimation faible et la réflexivité forte*, Systèmes d'information & management, Volume 15, mars 2010, pp. 41-70 [en ligne] (consulté le 20 août 2015) http://www.cairn.info/revue-systemes-d-information-et-management-2010-3-page-41.htm.

VERGÈS Étienne, *Preuve pénale : la géolocalisation face à l'article 8 de la CEDH*, Revue des droits et libertés fondamentaux, RDLF, chronique n°04, 2012 [en ligne] (consulté le 20 août 2015) http://www.revuedlf.com/droit-penal/preuve-penale-la-geolocalisation-face-a-l%E2%80%99article-8-de-la-cedh/.

FREYSSINET Eric, *Botnets : Illustration de nouvelles formes de criminalité organisée*, Revue du GRASCO, n°6, juillet 2013, pp. 10-18.

Myriam QUÉMÉNER, *Les spécificités juridiques de la preuve numérique*, AJ Pénal, 2014, p. 63.

Focus sur *La loi relative à la géolocalisation*, Dalloz Actu Etudiant, 11 avril 2014 [en ligne] (consulté le 20 août 2015) http://actu.dalloz-etudiant.fr.

HERRY Valentine et PÉCASTAING Juliette, *Les Bitcoins, nouvelle monnaie virtuelle : quels enjeux?*, Revue Sorbonne OFIS, octobre 2014, 4 pp..

GUINIER Daniel, *Monnaies virtuelles Le cas Bitcoin pourquoi tant d'emballement?*, Revue du GRASCO, n°12, avril 2015, pp. 37-52.

RAULT Raphaël, *Monnaie virtuelle et monnaie électronique : distinction et encadrement contractuel des porte-monnaie virtuels affectés*, LexisNexis, Tendance Droit, 28 juin 2015 [en ligne] (consulté le 20 août 2015) http://www.tendancedroit.fr/monnaie-virtuelle-et-monnaie-electronique-distinction-et-encadrement-contractuel-des-porte-monnaie-virtuels-affectes/.

DAOUD Emmanuel et PERONNE Géralsine, *Cyberattaques : la lutte s'intensifie*, AJ Pénal 2015, septembre 2015, p. 396.

- **Doctrine Internationale**

TREMBLAY Pierre, LAISNE Sylvie, CORDEAU Gilbert, SHEWSHUCK Angela et MCLEAN Brian, *Carrières criminelles collectives : évolution d'une population délinquante (groupes de motards)*, Criminologie, vol. 22, n° 2, 1989, pp. 65-94.

GALVES Fred, *Where the not-so-wild things are: Computers in the Courtroom, the Federal Rules of Evidence, and the Need for Institutional Reform and More Judicial Acceptance*, Harvard Journal of Law & Technology, Volume 13, n°2, 2000, pp. 165-302.

CHAWKI Mohamed, *Anonymity in Cyberspace: Finding the Balance between Privacy and Security*, Droit-Tic, juillet 2006, 24 pp..

SELINŠEK Liljana, *Electronic evidence in the Slovene Criminal Procedure Act*, Digital Evidence

and Electronic Signature Law Review, Volume 7, 2010, pp. 77-86.

ILIOUDIS Christos, MARTINI Adamantini, RACHAVELIAS Michael et ZAHARIS Alexandros, *Hiding illegal content in the swf format and spreading through social network services: a legal approach*, Digital Evidence and Electronic Signature Law Review, Volume 7, 2010, pp. 117-121.

VACIAGO Giuseppe, *Remote forensics and cloud computing: an italian and european legal overview*, Digital Evidence and Electronic Signature Law Review, Volume 8, 2011, pp. 126-129.

URBANO CASTRILLO (de) Eduardo, *The legal regulation of electronic evidence: A pending necessity*, Digital Evidence and Electronic Signature Law Review, Volume 8, 2011, pp. 25-32.

VANDENDRIESSCHE Johan, *The effect of 'virtual presence' in Belgium on the duty to cooperate with criminal investigations: some prudence may be required when confronted with a request from a Belgian public prosecutor*, Digital Evidence and Electronic Signature Law Review, Volume 8, 2011, pp. 194-195.

ŠEPEC Miha, *The trojan horse defence – a modern problem of digital evidence*, Digital Evidence and Electronic Signature Law Review, Volume 9, 2012, pp. 58-66.

BAGBY John et SCHWERHA Joseph, *International aspects of migrating digital forensics in the cloud*, Digital Evidence and Electronic Signature Law Review, Volume 10, 2013, pp. 81-96.

SKRTIC Drazen, *Electronic evidence and the Croatian Criminal Procedure Act*, Digital Evidence and Electronic Signature Law Review, Volume 10, 2013, pp. 128-135.

ŠEPEC Miha, *Digital data encryption – aspects of criminal law and dilemmas in Slovenia*, Digital Evidence and Electronic Signature Law Review, Volume 10, 2013, pp. 147-154.

A framework for a syllabus on electronic evidence, Digital Evidence and Electronic Signature Law Review, Volume 10, 2013, pp. 7-15.

SILVA RAMALHO David, *The use of malware as a means of obtaining evidence in Portuguese criminal proceedings*, Digital Evidence and Electronic Signature Law Review, Volume 11, 2014, pp. 55-75.

- **Presse Française**

GYORY Michel, *Le droit d'auteur face aux révolutions technologiques*, Revue en ligne Bon-A-Tirer, 2010 [en ligne] (consulté le 20 août 2015) http://www.bon-a-tirer.com/volume145/gyory.html.

CARIO Erwan, *L'attaque en déni de service, arme d'obstruction massive*, Libération Écrans, 10

décembre 2010 [en ligne] (consulté le 20 août 2015) http://ecrans.liberation.fr/ecrans/2010/12/10/l-attaque-en-deni-de-service-arme-d-obstruction-massive_953288.

BRAN Mirel, *Les pirates roumains d'"Hackerville" tiennent tête aux polices du monde entier*, Le Monde, 28 décembre 2011 [en ligne] (consulté le 20 août 2015) http://www.lemonde.fr/europe/article/2011/12/28/les-pirates-roumains-d-hackerville-tiennent-tete-aux-polices-du-monde-entier_1623331_3214.html.

WikiLeaks la Grande-Bretagne refuse que Julian Assange quitte son territoire, Le Monde, 16 août 2012 [en ligne] (consultés le 20 août 2015) http://www.lemonde.fr/technologies/article/2012/08/16/la-grande-bretagne-determinee-a-extrader-julian-assange_1746459_651865.html#v1Ob5YMwL0g7gTar.99.

La cybercriminalité coûte plus cher que les trafics de cocaïne, héroïne et marijuana, Le Monde, 8 mai 2012 [en ligne] (consulté le 20 août 2015) http://www.lemonde.fr/technologies/article/2012/05/08/la-cybercriminalite-coute-plus-cher-que-les-trafics-de-cocaine-heroine-et-marijuana_1698207_651865.html.

LAURENT Alexandre, *DDOS sans précédent contre Spamhaus : Internet va bien, merci pour lui*, CLUBIC, jeudi 28 mars 2013 [en ligne] (consulté le 20 août 2015) http://pro.clubic.com/it-business/securite-et-donnees/actualite-550362-spamhaus-ddos-cyberbunker.html.

ARÈNE Véronique, *Spamhaus victime d'une gigantesque attaque DDoS*, Le Monde Informatique, 28 mars 2013 [en ligne] (consulté le 20 août 2015) http://www.lemondeinformatique.fr/actualites/lire-spamhaus-victime-d-une-gigantesque-attaque-ddos-53029.html.

KALLENBORN Gilbert, *Monnaies virtuelles : un réseau de blanchiment mondial a été mis à jour*, 01net, 29 mai 2013 [en ligne] (consulté le 20 août 2015) http://www.01net.com/editorial/596389/monnaie-virtuelles-un-reseau-de-blanchiment-mondial-a-ete-mis-a-jour/#?xtor=EPR-1-[NL-01net-Actus]-20130529.

BARRERE Patrice, *Jeux en ligne. Les mafias entrent en jeu sur les paris sportifs*, Le Progrès, 11 juin 2013 [en ligne] (consulté le 20 août 2015) http://www.leprogres.fr/economie/2013/06/11/les-mafias-entrent-en-jeu-sur-les-paris-sportifs.

EUDES Yves et SEELOW Soren, *Le logiciel espion Blackshades au cœur d'une grande enquête internationale*, Le Monde, 23 mai 2014 [en ligne] (consulté le 20 août 2015) http://www.lemonde.fr/societe/article/2014/05/23/le-logiciel-espion-blackshades-au-coeur-d-une-grande-enquete-internationale_4424783_3224.html.

Ils enlèvent, séquestrent puis exigent une demandent de rançon à des Norvégiens : ça se passe à Dakar, Actusen, Société, 20 juin 2014 [en ligne] (consulté le 20 août 2015) http://www.actusen.com/ils-enlevent-sequestrent-puis-exigent-une-demandent-de-rancon-a-des-norvegiens-ca-se-passe-a-dakar/.

Droit à l'oubli: Google refuserait 60% des requêtes, L'Express – L'Expansion, 22 septembre 2014 [en ligne] (consulté le 20 août 2015) http://lexpansion.lexpress.fr/high-tech/droit-a-l-oubli-google-refuserait-60-des-requetes_1578114.html#gPhEOODw2cCGXcTr.99.

PONCET Guerric, *Europol a annoncé vendredi matin avoir mené une action coordonnée sur le continent européen. Les suspects sont essentiellement des « débutants »*, Le Point, 21 novembre 2014 [en ligne] (consulté le 20 août 2015) http://www.lepoint.fr/chroniqueurs-du-point/guerric-poncet/operation-mousetrap-lescybergendarmes-s-attaquent-aux-petits-criminels-du-net-21-11-2014-1883176_506.php.

MARVÃO Susana, *Plongée dans le monde des cybercriminels*, Revue Silicon, 2 décembre 2014 [en ligne] (consulté le 20 août 2014) http://www.silicon.fr/plongee-monde-cybercriminels-103081.html.

SENET Régis, *À TOR et à travers – Anonymat et utilisation malveillante*, XMCO, Revue ActuSecu, Numéro 39, janvier 2015, pp. 7-16.

GUIBERT Nathalie, LELOUP Damien et UNTERSINGER Martin, *Comment « Le Monde » a été piraté par l'Armée électronique syrienne*, Le Monde, 20 janvier 2015 [en ligne] (consulté le 20 août 2015) http://www.lemonde.fr/pixels/article/2015/01/20/comment-le-monde-a-ete-pirate-par-l-armee-electronique-syrienne_4559393_4408996.html.

DUCOURTIEUX Cécile, *Les Européens se fixent des règles pour lutter contre le blanchiment*, Le Monde, 27 janvier 2015 [en ligne] (consulté le 20 août 2015) http://www.lemonde.fr/europe/article/2015/01/27/les-europeens-se-fixent-des-regles-pour-lutter-contre-le-blanchiment_4564622_3214.html.

Des chercheurs créent un algorithme pour analyser les réseaux cybercriminels, Diplomatie digitale, 21 avril 2015 [en ligne] (consulté le 20 août 2015) http://www.diplomatie-digitale.com/featured/surete/influence-reseaux-cybercriminels-1626.

Des chercheurs créent un algorithme pour analyser les réseaux cybercriminels, Diplomatie digitale, 21 avril 2015 [en ligne] (consulté le 20 août 2015) http://www.diplomatie-digitale.com/featured/surete/influence-reseaux-cybercriminels-1626.

L'Elysée rejette la demande d'asile de Julian Assange, Le Monde, 3 juillet 2015 [en ligne]

(consultés le 20 août 2015) http://www.lemonde.fr/pixels/article/2015/07/03/l-elysee-rejette-la-demande-d-asile-de-julian-assange_4669082_4408996.html#CDErkX3H0wjA6Mkf.99.

Internet. Le piratage d'Ashley Madison révèle les limites de la vie privée en ligne, Courrier International, 20 août 2015 [en ligne] (consulté le 20 août 2015) http://www.courrierinternational.com/article/internet-le-piratage-dashley-madison-revele-les-limites-de-la-vie-privee-en-ligne.

- **Presse Internationale**

LEYDEN John, *Blue Security calls it quits after attack by renegade spammer - Folds spam fighting operation*, The Register, 17 mai 2006 [en ligne] (consulté le 20 août 2015) http://www.theregister.co.uk/2006/05/17/blue_security_folds/.

ZETTER. Kim, *Vigilantes Hack Criminal Carding Forum and expose underground dealings*, Wired, Security, 19 mai 2010 [en ligne] (consulté le 20 août 2015) http://www.wired.com/2010/05/carderscc/.

BHATTACHARJEE Yudhijit, *How a Remote Town in Romania Has Become Cybercrime Central*, Wired, Magazine, 31 janvier 2011 [en ligne] (consulté le 20 août 2015) http://www.wired.com/2011/01/ff_hackerville_romania/.

KUSHNER David, *Machine Politics - The man who started the hacker wars*, The New Yorker, Annals of Technology, 7 mai 2012 [en ligne] (consulté le 20 août 2015) http://www.newyorker.com/magazine/2012/05/07/machine-politics.

SINGER Natasha, *Mapping, and Sharing, the Consumer Genome*, The New Yorker, 16 juin 2012 [en ligne] (consulté le 20 août 2015) http://www.nytimes.com/2012/06/17/technology/acxiom-the-quiet-giant-of-consumer-database-marketing.html?_r=3&pagewanted=all.

GREENBERG Andy, *'Zerocoin' Add-on For Bitcoin Could Make It Truly Anonymous And Untraceable*, Forbes, 12 avril 2013 [en ligne] (consulté le 20 août 2015) http://www.forbes.com/sites/andygreenberg/2013/04/12/zerocoin-add-on-for-bitcoin-could-make-it-truly-anonymous-and-untraceable/.

KOPSTEIN Joshua, *Gold 2.0: can code and competition build a better Bitcoin? Zerocoin and Ripple present two ways to improve the ailing crypto-currency*, The Verge, 23 avril 2013 [en ligne] (consulté le 20 août 2015) http://www.theverge.com/2013/4/23/4252808/can-zerocoin-and-ripple-build-a-better-bitcoin.

LEWIS Helen, *Who are the trolls? - What we know about the men (and sometimes women) who spend their days trying to provoke a reaction on the internet*, New Statesman, 29 juillet 2013 [en ligne] (consulté le 20 août 2015) http://www.newstatesman.com/helen-lewis/2013/07/who-are-trolls.

KREBS Brian, *Russian internet payment boss sentenced*, The Age, 7 août 2013 [en ligne] (consulté le 20 août 2015) http://www.theage.com.au/it-pro/security-it/russian-internet-payment-boss-sentenced-20130805-hv179.

NESTLER (von) Franz, *Deutschland erkennt Bitcoins als privates Geld an*, Frantfurter Allgemeine Ginanzen, 16 août 2013 [en ligne] (consulté le 20 août 2015) http://www.faz.net/aktuell/finanzen/devisen-rohstoffe/digitale-waehrung-deutschland-erkennt-bitcoins-als-privates-geld-an-12535059.html.

HICKEN Melanie, *Find out what Big Data knows about you (it may be very wrong)*, CNN – Money, 5 septembre 2013 [en ligne] (consulté le 20 août 2015) http://money.cnn.com/2013/09/05/pf/acxiom-consumer-data/.

JACKSON HIGGINS Kelly, *Glut In Stolen Identities Forces Price Cut In Cyberunderground*, Information Week, Dark Reading, 19 novembre 2013 [en ligne] (consulté le 20 août 2015) http://www.darkreading.com/attacks-breaches/glut-in-stolen-identities-forces-price-cut-in-cyberunderground/d/d-id/1140914.

WESTIN Ken, *Stolen Target Credit Cards and the Black Market: How the Digital Underground Works*, The State of Security, 21 décembre 2013 [en ligne] (consulté le 20 août 2015) http://www.tripwire.com/state-of-security/vulnerability-management/how-stolen-target-credit-cards-are-used-on-the-black-market/

GREENBERG Andy, *The Dark Web Gets Darker With Rise of the 'Evolution' Drug Market*, Wired, 18 septembre 2014 [en ligne] (consulté le 20 août 2015) http://www.wired.com/2014/09/dark-web-evolution/.

OHLHORST Frank, *2015 prediction: Expect massive spikes in global information security threats*, TechRepublic, 19 novembre 2014 [en ligne] (consulté le 20 août 2015) http://www.techrepublic.com/article/2015-prediction-expect-massive-spikes-in-global-informationsecurity-threats/.

BOTEZATU Bogdan, *Five security scenarios to avoid this Christmas*, ABC, Technology and Games, 19 décembre 2014 [en ligne] (consulté le 20 août 2015) http://www.abc.net.au/technology/articles/2014/12/19/4152115.htm.

OHLHORST Frank, *Prevent 2015 from becoming another Year of the Data Breach*, TechRepublic, 11 décembre 2014 [en ligne] (consulté le 20 août 2015) http://www.techrepublic.com/article/prevent-2015-from-becoming-another-year-of-the-data-breach/.

NARAYAN Kaushik, *2014: The Year of the Data Breach – More Software Vulnerabilities and Breaches Than Any Year on Record*, Réseau Skyhigh, 2015 [en ligne] (consulté le 20 août 2015) https://www.skyhighnetworks.com/cloud-security-blog/2014-year-data-breach/.

JEONG Sarah, *The DHS Agent Who Infiltrated Silk Road to Take Down Its Kingpin*, Forbes, 15 janvier 2015 [en ligne](consulté le 20 août 2015) http://www.forbes.com/sites/sarahjeong/2015/01/14/the-dhs-agent-who-infiltrated-silk-road-to-take-down-its-kingpin/.

HILL Kashmir, *Future crime – These two Diablo III players stole virtual armor and gold — and got prosecuted IRL*, 20 mai 2015, Fusion [en ligne] (consulté le 20 août 2015) http://fusion.net/story/137157/two-diablo-iii-players-now-have-criminal-records-for-stealing-virtual-items-from-other-players/.

DUNE Lawrence, Bloomberg Business, 18 juin 2015, *The Hunt for the Financial Industry's Most-Wanted Hacker* [en ligne] (consulté le 10 août 2015) http://www.bloomberg.com/news/features/2015-06-18/the-hunt-for-the-financial-industry-s-most-wanted-hacker.

ELGOT Jessica, HERN Alex et WEAVER Matthew, *Ashley Madison adultery site hack: will I be found out?*, The Guardian, 21 juin 2015 [en ligne] (consulté le 20 août 2015) http://www.theguardian.com/world/2015/jul/21/ashley-madison-adultery-site-hack-will-i-be-found-out-what-you-need-to-know.

TIMBERG Craig, *A disaster foretold, and ignored - LOpht's warnings about the Internet drew notice but little action*, The Washington Post, 22 juin 2015 [en ligne] (consulté le 20 août 2015) http://www.washingtonpost.com/sf/business/2015/06/22/net-of-insecurity-part-3/.

HACKETT Robert, *Why your bank may not care if your credit card was hacked*, Fortune, 26 juin 2015 [en ligne] (consulté le 20 août 2015) http://fortune.com/2015/06/26/bank-credit-card-hack/.

YADRON Danny, *Cyberattack could expose millions of users' personal information*, Wall Street Journal, 20 juillet 2015 [en ligne] (consulté le 20 août 2015) http://www.wsj.com/articles/affair-website-ashley-madison-hacked-1437402152.

Le collectif Rex Mundi a dérobé les données de 24.000 clients de la société AFC, Sud Info, 20 juillet 2015 [en ligne] (consulté le 20 août 2015) http://www.sudinfo.be/1336319/article/2015-07-20/le-collectif-rex-mundi-a-derobe-les-donnees-de-24000-clients-de-la-societe-afc.

Séquestration et demande de rançon - La Dic démantèle un réseau de cybercriminels nigérians à Nord-Foire, Thies Vision, 21 août 2015 [en ligne] (consulté le 20 août 2015) http://www.thiesvision.com/Sequestration-et-demande-de-rancon-La-Dic-demantele-un-reseau-de-cybercriminels-nigerians-a-Nord-Foire_a12436.html.

DOCUMENTATION DES ACTEURS PRIVÉS

ROYAKKERS Lambèrs et WEL (van) Lita, *Ethical issues in web data mining*, Ethics and Information Technology, n°6, 2004, pp. 129-140.

Laboratoire d'EXpertise en Sécurité Informatique, *Cybercriminalité des Jeux en Ligne*, Livre Blanc du CERT-LEXSI, juillet 2006, 21 pp..

Group-IB, *State and trends of the "Russian" digital crime market*, 2011, 32 pp..

TISSIER Guillaume (dir.), Étude *Les marches noirs de la cybercriminalité*, Compagnie Européenne d'Intelligence Stratégique (CEIS), Collection Notes Stratégiques, Technologies de l'information, équipe Secu-Insight de CEIS, juin 2011, 73 pp..

PAGET François et SAMANI Raj, *Cybercrime Exposed – Cybercrime-as-a-Service*, McAfee Labs, 2013, 18 pp..

Le Cloud et le Big Data annoncent le retour en grâce de la donnée consommateur, document AC-0876-13 6/13 ACXIOM, 2013 [en ligne] (consulté le 20 août 2015) http://www.acxiom.fr/ressources/le-cloud-et-le-big-data-annoncent-le-retour-en-grace-de-la-donnee-consommateur/.

HART Matthew, PAGET François, SAMANI Raj, *Le blanchiment numérique Analyse des monnaies virtuelles et de leur utilisation à des fins criminelles*, McAfee Labs, 2013, Livre blanc, 17 pp..

EVEN Maxence, GREY Aude et LOUIS-SIDNEY Barbara, Étude *Monnaies virtuelles et cybercriminalité Etat des lieux et perspectives*, Compagnie Européenne d'Intelligence Stratégique (CEIS), Collection Notes Stratégiques, Technologies de l'information, 10 avril 2014, 48 pp..

Net Losses: Estimating the Global Cost of Cybercrime - Economic impact of cybercrime II, Center for Strategic and International Studies et MacAfee, juin 2014, 24 pp..

JENKINS Quentin, *Second arrest in response to DDoS attack on Spamhaus*, Spamhaus, 7 juillet 2014 [en ligne] (consulté le 20 août 2015) http://www.spamhaus.org/news/article/715/second-arrest-in-response-to-ddos-attack-on-spamhaus.

DIALLO Ismaila, *Un profil des marchés criminels à Dakar*, Rapport 264, Institut d'Études de Sécurité (ISS), août 2014, 12 pp..

Underground Hacker Markets, DELL Secure Works, décembre 2014, 16 pp..

HARBISON Cammy, *10 Largest Data Breaches Of 2014; The Sony Hack Is Not One Of Them*, 26 décembre 2014, iDigital Times [en ligne] (consulté le 20 août 2015) http://www.idigitaltimes.com/10-largest-data-breaches-2014-sony-hack-not-one-them-403219.

DOCUMENTATION OFFICIELLE

- **Union Internationale des Communications**

ITU, Secteur du développement des télécommunications, *Comprendre la cybercriminalité – Phénomène, difficultés et réponses juridiques*, Genève, septembre 2012, p. 241.

- **Interpol**

Interpol, *INTERPOL-coordinated operation strikes back at 'sextortion' networks*, 2 mai 2014 [en ligne] (consulté le 10 août 2015) http://www.interpol.int/News-and-media/News/2014/N2014-075.

Interpol, *INTERPOL coordonne une opération mondiale visant à mettre le botnet Simda hors d'état de nuire*, Singapour, 13 avril 2015 [en ligne] (consulté le 20 août 2015) http://www.interpol.int/fr/Centre-des-médias/Nouvelles/2015/N2015-038.

- **ICANN**

ICANN, *Suppression du registraire EstDomains*, 11 décembre 2008 [en ligne] (consulté le 20 août 2015) https://www.icann.org/news/announcement-2008-11-12-en.

- **Conseil de l'Europe**

Conseil de l'Europe, *Rapport explicatif sur la Convention sur la cybercriminalité*, STE n°185, 8 novembre 2001 [en ligne] (consulté le 21 août 2015)

http://conventions.coe.int/Treaty/FR/Reports/Html/185.htm.

Conseil de l'Europe, *Défis de l'accès de la justice pénale aux données stockées dans le nuage*, Document de réflexion T-CY (2015)10, Comité de la Convention sur la cybercriminalité, Groupe sur les preuves dans le nuage, Strasbourg (France), 26 mai 2015, 25 pp. [en ligne] (consulté le 20 août 2015) https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016803053cb.

- **Union européenne**

Commission Européenne, *Communication COM(2004) 28 final sur les communications commerciales non sollicitées ou "spam"*, 22 janvier 2004 [en ligne] (consulté le 20 août 2015) http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=celex:52004DC0028.

Commission Européenne, *Les pays européens s'allient pour combattre le "spamming" (envoi non sollicité de courriels)*, IP/05/146, Bruxelles, 7 février 2005 [en ligne] (consulté le 20 août 2015) http://europa.eu.int/information_society/topics/ecomm/highlights/current_spotlights/spam/index_en.htm.

Commission Européenne, *Rapport de la Commission - Deuxième rapport fondé sur l'article 14 de la décision-cadre du Conseil du 28 mai 2001 concernant la lutte contre la fraude et la contrefaçon des moyens de paiement autres que les espèces {SEC(2006) 188}*, Communication COM/2006/0065 final.

European Gaming and Betting Association (EGBA), Factsheet *Anti blanchiment d'argent*, 23 juillet 2010 [en ligne] (consulté le 20 août 2015) http://www.egba.eu/pdf/EGBA_FS_MoneyLaundering_french.pdf.

Parlement Européen, *Taxer les jeux d'argent en ligne pour lutter contre les activités de la mafia*, Communiqué de presse n°20121112IPR55400, Commission spéciale sur la criminalité organisée, la corruption et le blanchiment de capitaux, 12 novembre 2012, 2 pp..

Parlement Européen, *Réponse donnée par Mme Reding au nom de la Commission*, Question parlementaire P-000873/2013, 12 mars 2013 [en ligne] (consulté le 20 août 2015) http://www.europarl.europa.eu/sides/getAllAnswers.do?reference=P-2013-000873&language=FR.

Eurojust, *Rapport annuel pour 2014*, La Haye, Pays-Bas, 2015, 76 pp. [en ligne] (consulté le 27 septembre 2015) http://www.eurojust.europa.eu/doclibrary/corporate/eurojust%20Annual%20Reports/Annual%20Report%202014/Annual-Report-2014-FR.pdf.

Banque Centrale Européenne, *Virtual currency schemes – a further analysis*, février 2015, 37 pp..

Commission Européenne, *Data protection Eurobarometer out today*, 24 juin 2015 [en ligne] (consulté le 20 août 2015) http://ec.europa.eu/justice/newsroom/data-protection/news/240615_en.htm.

Eurojust, « *US Attorney General Lynch announces Cyber Prosecutor at Eurojust* », La Haye, 16 septembre 2015 [en ligne] (consulté le 27 septembre 2015) http://www.eurojust.europa.eu/press/PressReleases/Pages/2015/2015-09-16.aspx.

- **France**

Cour de cassation, LEMOINE Pascal, *La loyauté de la preuve (à travers quelques arrêts récents de la chambre criminelle)*, Études, 2004 [en ligne] (consulté le 20 août 2015) https://www.courdecassation.fr/publications_26/rapport_annuel_36/rapport_2004_173/deuxieme_partie_tudes_documents_176/tudes_diverses_179/travers_quelques_6401.html.

Sénat Français, Commission des Finances, du contrôle budgétaire et des comptes économiques de la Nation, TRUCY François, *L'évolution des jeux de hasard et d'argent*, Rapport d'information n°58, 7 novembre 2006.

Ministère de la Culture et de la Communication, France, *Le « spam »*, 13 parties, 4 avril 2007 [en ligne] (consulté le 20 août 2015) http://www.culturecommunication.gouv.fr/Politiques-ministerielles/Industries-culturelles/Dossiers-thematiques/Le-spam.

Assemblée nationale, Commission des finances, de l'économie générale et du contrôle budgétaire, FILIPPETTI Aurélie et LAMOUR Jean-François, *Mise en application de la loi n° 2010-476 du 12 mai 2010 relative à l'ouverture à la concurrence et à la régulation du secteur des jeux d'argent et de hasard en ligne*, Rapport d'information n°3463, 25 mai 2011 [en ligne] (consulté le 20 août 2015) http://www.assemblee-nationale.fr/13/rap-info/i3463.asp.

CNIL, *Le numéro IP*, 30 novembre 2011 [en ligne] (consulté le 20 août 2015) http://www.cil.cnrs.fr/CIL/spip.php?article1463.

Ministère de l'Intérieur, *Qu'est-ce-que la cybercriminalité?*, 1er février 2012 [en ligne] (consulté le 20 août 2015) http://www.interieur.gouv.fr/A-votre-service/Ma-securite/Conseils-pratiques/Sur-internet/Qu-est-ce-que-la-cybercriminalite.

Autorité de régulation des jeux en ligne (ARJEL), *Rapport d'activité 2013*, 2014, 49 pp. [en ligne] (consulté le 20 août 2015) http://www.arjel.fr/IMG/pdf/rapport-interactif-2013.pdf.

Cellule de traitement des informations financières (CTIF), DELEPIÈRE Jean-Claude, *21ème Rapport d'activités*, Belgique, Bruxelles, 2014, 108 pp..

Groupe de travail interministériel sur la lutte contre la cybercriminalité, *Protéger les internautes – Rapport sur la cybercriminalité*, février 2014, 277 pp..

Ministère des Finances et des Comptes publics, TRACFIN, Groupe de travail « Monnaies virtuelles », *L'encadrement des monnaies virtuelles – Recommandations visant à prévenir leurs usages à des fins frauduleuses ou de blanchiment*, juin 2014, 10 pp..

Note du Centre de Recherche de l'École des Officiers de la Gendarmerie Nationale (CREOGN), France, *Monnaies virtuelles : nature et risques*, septembre 2014, Note numéro 6, 4 pp..

Observatoire des jeux, France, COSTES Jean-Michel, EROUKMANOFF Vincent, RICHARD Jean-Baptiste, TOVAR Marie-Line, *Notes sur les jeux d'argent en France en 2014*, Les notes de l'Observatoire des jeux, n° 6, avril 2015, 9 pp..

- **Canada**

Gendarmerie royale du Canada, Direction des services de police communautaires, contractuels et autochtones, Sous-direction de la recherche et de l'évaluation, LEMIEUX Vincent, *Les réseaux criminels*, Ottawa, mars 2003, 26 pp.

Centre d'analyse des opérations et déclarations financières du Canada (CANAFE), *Tendances et typologies en matière de blanchiment d'argent dans le secteur canadien des valeurs mobilières*, Rapports de typologies et tendances, avril 2013, « Risques supplémentaires - le courtage en ligne », 25 pp. [en ligne] (consulté le 20 août 2015) http://www.fintrac.gc.ca/publications/typologies/2013-04-fra.pdf.

- **États-Unis**

United States Computer Emergency Readiness Team (US-CERT), DESANTIS Matthew, DOUGHERTY Chad, MCDOWELL Mindi, *Understanding and Protecting Yourself Against Money Mule Schemes*, 22 juin 2012 [en ligne] (consulté le 20 août 2015) https://www.us-cert.gov/security-publications/understanding-and-protecting-yourself-against-money-mule-schemes.

Département du Commerce, National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, 12 février 2014, 39 pp..

Département de la Justice, Bureau des affaires publiques, *Russian National Charged in Largest Known Data Breach Prosecution Extradited to United States*, 17 février 2015 [en ligne] (consulté le 20 août 2015) http://www.justice.gov/opa/pr/russian-national-charged-largest-known-data-breach-prosecution-extradited-united-states.

Département d'État, *Programme de primes contre le crime organisé transnational* [en ligne] (consulté le 20 août 2015) http://www.state.gov/j/inl/tocrewards/.

SITES INTERNET

Association Eco https://www.eco.de.

Centre National de Ressources Textuelles et Lexicales (CNRTL) www.cnrtl.fr.

Dictionnaire Larousse www.larousse.fr.

Ebay www.pages.ebay.fr.

EGEDIAN www.egedian.com.

Facebook www.facebook.com.

Fondation Wikimedia www.wikimediafoundation.org.

Internet Watch Foundation (IWF) www.iwf.org.uk.

The TOR Project www.torproject.org.

Twitter www.support.twitter.com.

Vade-Retro www.vade-retro.com.

MoneyGram www.moneygram.fr.

Site d'entraînement au *hacking* www.hackbbs.org.

Fondation CEATA www.ceata.org/.

VIDÉOS

- **Documentaires**

DUNNE Sean, « The most dangerous town on the Internet », Norton Symantec, 19,59 minutes [en ligne] (consulté le 20 août 2015) http://us.norton.com/mostdangeroustown/index.html#!/en-US.

BRAN Mirel, « Roumanie : "Hackerville", capitale de l'arnaque sur Internet », France 24, 17

minutes [en ligne] (consulté le 20 août 2015) http://www.dailymotion.com/video/xvof5p_roumanie-hackerville-capitale-de-l-arnaque-sur-internet_news.

- **Films**

« War Games », de John Badham, 1993 (États-Unis).

« Die Hard 4 Retour en Enfer », de Len Wiseman, 2007 (États-Unis).

Lexique

- A -

Administrateur

1. Dans un jeu en ligne, l'administrateur est un individu qui a le pouvoir d'édicter et modifier les règles du jeu (naturelles et positives). Il assure la gouvernance économique et financière (émission de monnaie, régulation du marché des changes), il détient le pouvoir de punir (par le bannissement temporaire, la confiscation des biens, la rétrogradation d'un ou plusieurs niveaux, la suppression de l'avatar et la clôture du compte) et le pouvoir de surveillance et de contrôle (surveillance et censure).

2. Sur un site Internet, ce terme désigne tout utilisateur membre du groupe des administrateurs, appartenance qui lui garantit certains privilèges, tenant à la gestion des signalements, à la surveillance des publications, à la censure des contenus et à l'exclusion des utilisateurs dont le comportement est jugé inadéquat.

3. L'administrateur système est l'individu responsable des aspects techniques. Il doit s'assurer que le système informatique est utile et économique. Celui-ci peut être un réseau, le système de gestion d'une base de données ou une machine animant un ou plusieurs services.

→ Voir **Avatar**, **Gamer** et **MMORPG**.

Altcoins

« *Altcoin* » est un néologisme anglais, abrégeant les termes « *alternative coin* ». Il désigne toute crypto-monnaie inspirée de *Bitcoin*. Ces monnaies alternatives visent généralement la correction des défauts perçus de *Bitcoin*. Ce sont des monnaies pair à pair impliquant le minage et des transactions bon marché sur Internet.

→ Voir **Crypto-monnaie** et **Pair à pair**.

Antis

Sous le terme « antis », les spammeurs regroupent tous les opposants au *spam* de la société civile, qu'ils agissent seuls ou de conserve avec d'autres pour entraver ou démanteler les opérations de *spamming* à grande échelle.

→ Voir **Spam**.

Antisec

Le mouvement *antisec* regroupe des *hackers* et des spécialistes de la sécurité informatique opposés à ce que les failles de sécurité soient rendues publiques.

→ Voir **Faille**, **Full disclosure** et **Zero Day**.

Appairage

L'appairage (« *peering* » en Anglais) en informatique est la pratique ayant cours entre les fournisseurs d'accès à Internet (FAI) et de services (FSI) d'échanger du trafic Internet.

→ Voir **Fournisseur d'accès Internet** et **Fournisseur de services Internet**.

Attaque informatique

Ce terme générique désigne toute action malveillante dont la cible ou le moyen est informatique et qui génère un dommage ou un préjudice. L'agresseur exploite souvent une vulnérabilité dans un logiciel ou un système de sécurité pour installer un *malware*, qui récupère et transmet des données ou développe une autre attaque interne, pour bloquer ou saboter le réseau ou le terminal, par exemple.

→ Voir **Black hat**, **Cheval de Troie**, **Code source**, **Cracker**, **DDoS**, **Exploit kit**, **Faille**, **Malware**, **Piratage de site** et **Virus informatique**.

Avatar

Un avatar est la représentation virtuelle que l'utilisateur d'un système informatique choisit pour le représenter graphiquement, souvent dans un jeu électronique ou pour ses communications électroniques. Le terme vient de la tradition hindoue où il désigne l'incarnation terrestre d'une divinité.

→ Voir **Administrateur**, **MMORPG** et **Gamer**.

- B -

Big data

Ce terme anglais, signifiant littéralement « grosse donnée », est un concept popularisé en 2012 pour faire référence à l'explosion du volume des données dans l'entreprise et de la nécessité de recourir sans cesse à de nouvelles approches technologiques pour stocker, traiter et utiliser ces volumes « critiques ».

Le phénomène est devenu un enjeu commercial et économique majeur, aussi bien que technique. L'expression *big data* désigne aussi les nouveaux moyens de stockage, traitement et utilisation des données qui ont été créés pour y faire face. Ils se démarquent très nettement sur la « Vénérable grille de lecture » établie en 2001 par Doug Laney du cabinet Gartner, les trois V du *Big Data* : volume (des échanges), variété (des sources et des contenus) et vélocité (collecte et traitement en temps réel).

Occasionnellement, les analystes signalent que cette révolution de la donnée impacte négativement d'autres dimensions : la validité, la véracité, la valeur ou la visibilité des données.

→ Voir **Donnée**, **Donnée personnelle**, **Données propriétaires** et **Données publiques**.

Black hat

Créateurs de virus, cyber-espions, cyber-terroristes ou cyber-escrocs, ils agissent la plupart du temps hors-la-loi, dans le but de nuire, de faire du profit ou d'obtenir des informations. Ces *hackers* n'ont pas la même éthique que les *white hats* et sont souvent malveillants. Les pires sont appelés *crashers*, ils ne visent que la destruction.

En Français, on pourra d'ailleurs les appeler « pirates » ou « assaillants malveillants ».

→ Voir **Piratage de site** et **White hat**.

Blue hat

Ce terme désigne certains consultants en sécurité informatique, *hackers* et ingénieurs en sécurité, chargés de vérifier l'absence de *bugs* et de corriger d'éventuels *exploits* avant le lancement d'un système d'exploitation sur le marché, notamment ceux qu'emploie Microsoft pour détecter d'éventuelles vulnérabilités.

→ Voir **Bug**, **White hat**.

Black SEO

SEO est l'acronyme de « *search engine optimization* ». Il s'agit d'un ensemble de méthodes, techniques et stratégies servant à augmenter le trafic Internet d'un site en lui assurant un excellent référencement sur les moteurs de recherche (Google, Bing, Yahoo, etc).

La *black SEO* est le fait d'abuser de la *SEO* en manifestant une agressivité excessive. Les termes « *spamdexing* » ou « référencement abusif » sont utilisés comme synonymes. Certaines tactiques lui sont spécifiques, comme le *cloaking*, les *link farms* ou encore le *keyword stuffing*.

Le *cloaking* (du terme anglais « dissimulation ») est une technique consistant pour un serveur Internet à présenter une page web différente suivant que le client distant est un robot de moteur de recherche ou un internaute humain. Dans la technique des *link farms*, de multiples sites ou pages se référencent mutuellement. Souvent, les sites utilisent des robots pour poster des liens les référençant sur des forums ou, sinon, une page Internet satellite (ou *doorway page*) améliore le référencement en proposant de nombreux liens vers le site, associés à des combinaisons de mots-clés conçues pour obtenir un score élevé lors de l'évaluation par les algorithmes des moteurs de recherche. Le bourrage de mots-clés (*keyword stuffing*) est la conception d'une page truffée de mots-clés destinés à être référencés.

→ Voir **Hébergeur bulletproof** et **Moteur de recherche**.

Bug

Ce terme anglais désigne normalement un insecte. Il désigne aujourd'hui les problèmes critiques dont peut souffrir un programme. Le *bug* recouvre à la fois l'erreur de programmation insérée dans le code source du programme et le comportement aberrant qui en résulte. La recherche de cette faute de codage initiale est appelée débogage.

La désignation a été étendue aux problèmes de *software* car, selon la légende, les tout premiers ordinateurs, qui occupaient des pièces entières, dysfonctionnaient souvent à cause des insectes, lesquels venaient se perdre dans leurs circuits et brûler. Curieusement, une inversion s'est produite par la suite : de tels soucis matériels sont appelés « *glitch* », ou « pépin », alors que seuls les problèmes de code sont appelés *bug*. Ce dernier terme a été francisé sous la forme de « bogue », qui est un masculin, dans ce contexte, contrairement au terme désignant la coque d'une châtaigne.

→ Voir **Glitch**, **Hardware** et **Software**.

- C -

Carding

Cette appellation englobe toutes les fraudes de cartes de débit et de crédit en ligne.

→ Voir **Skimmer**.

Cheval de Troie

Ce programme malveillant, nommé par référence à la chute de Troie, lui permet de prendre

le contrôle d'un ordinateur et/ou de s'en servir à l'insu du propriétaire. Le logiciel paraît inoffensif mais il contient une fonction illicite cachée et connue du seul attaquant. En effet, le programme est généralement installé sans qu'il le sache par l'utilisateur lui-même.

→ Voir **Malware** et **RAT**.

Cloud computing

Le *cloud computing*, parfois traduit littéralement « informatique en nuage », « nuagique » ou encore « infonuagique », est une forme de délocalisation de l'infrastructure informatique permettant d'accéder à des ressources informatiques, à la demande et en libre-service. Il exploite la puissance de calcul ou de stockage de serveurs informatiques distants par l'intermédiaire d'un réseau, généralement Internet.

Code source

Le code source d'un logiciel est un ensemble d'instructions écrites dans un langage de programmation informatique. Il prend la forme d'un texte lisible par un utilisateur.

Codeurs

Les codeurs sont des pirates capables de créer leurs propres outils d'intrusion, par opposition aux *script kiddies*. Ils sont l'équivalent des programmeurs informatiques dans le monde du *hacking*, bien qu'ils puissent ne pas avoir reçu une éducation formelle.

→ Voir **Exploit kit**, **Hacker** et **Script kiddies**.

Contrat de licence d'utilisateur final (CLUF)

Mieux connu sous l'acronyme « CLUF », ce contrat est le document que l'utilisateur doit signer pour installer un programme et qui protège son concepteur, en évitant notamment qu'il ne soit utilisé pour plus longtemps que ne le prévoyait le contrat de location, qu'il serve un propos qui n'était pas prévu ou encore que l'utilisateur le copie.

Cookie

Ce fichier témoin, installé sur le disque dur d'un internaute à l'occasion de la consultation de certains sites, permet à son expéditeur de collecter des données comportementales sur l'utilisateur et de le reconnaître lors de son passage suivant sur le site. Il peut ainsi lui éviter d'entrer à nouveau ses identifiants de connexion.

Courrier électronique

Il s'agit de tout message envoyé par un réseau de communication, stocké sur un serveur du

réseau ou dans l'équipement terminal du destinataire, jusqu'à ce que ce dernier le récupère. Des synonymes existent, comme « *e-mail* », « *mail* », « mel » ou « courriel ».

Courtier en données

Les courtiers en données, ou courtiers en informations (*data brokers* ou *information brokers* en Anglais), se définissent principalement par leur activité, qui consiste à recueillir et à vendre des renseignements personnels. Bien qu'il s'agisse de données personnelles, dans l'immense majorité des cas, ils ne respectent pas les exigences de transparence qui devraient s'attacher à leur collecte. Il existe néanmoins des exceptions. Il s'agira tantôt d'organisations, tantôt d'individus. Malgré leur mauvaise réputation, ils procurent essentiellement des services bénins, participant au ciblage du marketing comme à la mise à jour des fichiers consommateurs.

→ Voir **Donnée**, **Donnée personnelle**, **Données propriétaires**, **Données publiques, Doxxing et Fouille de données**.

Courtier en bourse

La traduction anglaise du terme, « *broker* » est utilisée comme synonyme. Traditionnellement, le courtier est la personne qui sert d'intermédiaire dans des opérations commerciales ou autres, contre une rémunération qui prend généralement la forme d'une commission. Dans la plupart des pays, dont la France, l'activité de courtage est réglementée.

Le courtier gère le compte de *trading* des opérateurs et investisseurs sur les marchés financiers (exécutions des ordres d'entrée et de sortie du marché, etc). Avec le développement du *trading* en ligne, le recours à un courtier pour accélérer les transactions s'est généralisé.

Cracker

Les programmeurs, qui se considèrent comme des *hackers* eux-mêmes, appellent ainsi les *black hats*. Le terme *cracker* était pourtant initialement plutôt positif, qualifiant des utilisateurs curieux démantelant les programmes et systèmes sans causer de préjudices.

→ Voir **Black hat** et **Hacker**.

Crime organisé (pirates du)

Un certain nombre de grandes familles du crime organisé emploient des criminels qui utilisent essentiellement ou exclusivement l'outil informatique.

Cryptage de données

Le cryptage de données est un processus informatique rendant les informations indéchiffrables. Il permet de protéger les données d'un utilisateur contre les lectures et les utilisations non autorisées.

Il sert aussi à la sécurisation de certaines opérations en ligne, bancaires par exemple. Il existe d'autres procédés servant le même propos, comme l'ajout d'un paramètre de vérification. Il peut s'agir de répondre à une question de sécurité (date de naissance, premier animal de compagnie, etc) ou de fournir un code dynamique.

Crypto-monnaie

Une crypto-monnaie est une monnaie électronique pair à pair et décentralisée dont l'implémentation se base sur les principes de la cryptographie pour valider les transactions et la génération autonome de la monnaie. Les implémentations des crypto-monnaies utilisent un système de preuve de travail pour les protéger des contrefaçons électroniques. La plupart des crypto-monnaies sont conçues pour introduire graduellement de nouvelles unités de monnaie, dans la limite d'un total raisonnable de monnaie en circulation.

→ Voir **Altcoins** et **Pair à pair**.

Cybercriminalité

Ce phénomène criminel recouvre toutes les infractions strictement informatiques ciblant des systèmes d'information, des systèmes de traitement informatisé des données, ainsi que des infractions classiques, comme les fraudes et les escroqueries facilitées ou démultipliées par le recours à Internet.

→ Voir **STAD**.

Cyberespace

C'est l'espace de communication constitué par l'interconnexion mondiale d'équipements de traitement automatisé de données numériques.

→ Voir **World Wide Web**.

Cybersquattage

L'anglicisme « *cybersquatting* », utilisé plus fréquemment, est une pratique consistant à enregistrer un nom de domaine correspondant à une marque ou une personne, avec l'intention de le revendre ensuite à l'ayant-droit, d'altérer sa visibilité ou de profiter de sa

notoriété.

Les cybersquatteurs mettent cette manœuvre à exécution avant que l'ayant-droit ait déposé le nom de domaine ou après s'il a oublié de le renouveler. Un cas particulier est celui du *typosquatting*, l'utilisation d'un nom de domaine connu avec une faute minime, qui permet de détourner des visiteurs égarés. Ils peuvent le faire une fois contre une seule marque ou procéder à des enregistrements massifs.

Pour certaines lois ou jurisprudences locales, il s'agit d'une extorsion ou de parasitisme. La législation française, par exemple, considère le *cybersquatting* comme une forme de contrefaçon, le recours à la Justice pour se réapproprier un nom de domaine qui devrait nous appartenir est toujours possible, bien qu'un peu coûteux. Aux États-Unis, suivant le *Truth in Domain Names Act* de 2003, cette pratique peut être punie d'un maximum de deux ans de prison et d'amendes pouvant aller jusqu'à 100.000 dollars.

→ Voir **Nom de domaine**.

- D -

Darknets

Ce sont des réseaux d'échange de fichiers en ligne qui assurent l'anonymat aux utilisateurs au moyen de technologies de chiffrement et de cybersécurité. Ils permettent aux criminels de négocier leurs produits et services illégaux sur Internet et d'éviter d'être repérés sur des réseaux anonymes. Ils font le jeu des délinquants, qui s'en servent pour toutes les transactions illégales. Lorsqu'ils sont utilisés

→ Voir **Deep web** et **TOR**.

DDoS

L'attaque par déni de service distribué (*distributed denial of service attack*) est une variante de l'attaque par déni de service (*denial of service attack*). C'est une attaque informatique ayant pour but de rendre indisponible un système informatique, d'empêcher les utilisateurs légitimes d'un service de l'utiliser.

Le déni de service distribué, provoqué par des programmes simultanément activés sur plusieurs machines attaquantes, souvent membres d'un *botnet*, peut paralyser un ou plusieurs sites, programmes ou connexions.

→ Voir **Attaque informatique** et **Zombies**.

Déréférencement

Le déréférencement est l'action qui consiste à supprimer des résultats d'un moteur de recherche un site Internet ou une page web.

→ Voir **Moteur de recherche**.

Deep web

Signifiant littéralement « la toile profonde », ce terme recouvre la partie d'Internet qui est accessible en ligne, mais pas indexée dans les moteurs de recherche classiques.

→ Voir **Cyberespace**, **Darknets**, **TOR** et **World Wide Web**.

Dictionnaire

L'attaque par dictionnaire, utilisée en cryptanalyse pour trouver un mot de passe ou une clé, consiste à tester une série de mots de passe potentiels successivement dans l'espoir que le mot de passe utilisé pour le chiffrement soit contenu dans le dictionnaire. Sinon, l'attaque échouera.

L'attaque par dictionnaire complète bien les attaques par force brute, qui consistent à tester toutes les différentes possibilités de mots de passe. Cette dernière n'est efficace que si le nombre de caractères est déjà défini et n'excède pas la demi-douzaine.

L'attaque d'annuaire est une technique d'envoi de pourriels basée sur la génération d'adresses électroniques par une méthode mélangeant force brute basée sur une simple attaque par dictionnaire et attaque par dictionnaire : plutôt que de simples caractères, elle va combiner des lettres, des prénoms, des noms de famille courants et des noms communs.

→ Voir **Courrier électronique** et **Spam**.

Donnée

Il s'agit de toute représentation d'une information sous une forme conventionnelle destinée à faciliter son traitement.

→ Voir **Ouverture des données** et **STAD**.

Donnée personnelle

Il s'agit de toute information relative à une personne physique identifiée ou susceptible de l'être, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres.

Données propriétaires

Cette traduction littérale de l'anglais « proprietary information » peut être utilisée de préférence aux termes « renseignements confidentiels » ou « renseignements exclusifs ».

Elle désigne des données qui ne sont pas du domaine public et qui sont traitées comme si elles appartenaient à leur détenteur. Généralement, ce terme est employé lorsque les données sont partagées avec d'autres personnes. Celles-ci peuvent avoir le consentement du détenteur, et alors on sera souvent face à des intermédiaires de collecte ou de traitement de ces données, généralement tributaires de l'objectif dans lequel ils ont été autorisés à accéder à l'information. Elles peuvent aussi se les procurer à l'insu du détenteur ou à l'encontre de sa volonté.

Un tel accès est interdit par la plupart des législateurs lorsqu'il s'agit de secrets industriels ou commerciaux. Aux États-Unis, c'est le cas depuis 1996 et l'entrée en vigueur du *Economic Espionage Act of 1996* (EEA).

→ Voir **Données publiques**.

Données publiques

Les données publiques sont toutes les données recueillies, maintenues et utilisées par les organismes publics.

→ Voir **Données propriétaires**.

Doxxing

Le *doxxing* est à distinguer du *doxing*, lequel désigne simplement la publication d'informations dans un document (« doc » ou « dox » en abrégé). Le *doxxing* vise à nuire à

une entité en procédant au *doxing* d'informations confidentielles ou personnelles.

Dans une autre interprétation, le *doxing* est le fait de recueillir, sur demande, un maximum d'information sur une personne physique ou morale.

- E -

Elite hacker

Il s'agit d'un *hacker* de grand talent, généralement membre d'un ou plusieurs groupes partageant les plus récents *exploits*.

→ Voir **Hacker**.

Escrow

L'*escrow* est un tiers de confiance indépendant qui, dans le cadre d'une procédure de dépôt fiduciaire (en Anglais, « *escrow payment* »), servira d'intermédiaire dans une transaction, recevant et transmettant l'argent ou les documents concernés. La plupart des marchés noirs de la cybercriminalité offre leurs services comme *escrows*.

→ Voir **Darknets** et **Smurfer**.

Exploit kit

L'*exploit kit* est un ensemble d'*exploits*, des programmes permettant à un *hacker* d'automatiser l'exploitation d'une vulnérabilité dans un programme existant. Les *script kiddies* en sont friands. Ils sont principalement utilisés pour mener à bien des attaques automatisées afin de propager des programmes malveillants.

→ Voir **Codeur**, **Faille**, **Script kiddies** et **Zero Day**.

- F -

Faille

La faille est la vulnérabilité d'un système informatique qui permet de porter atteinte à son fonctionnement normal, à la confidentialité ou à l'intégralité des données qu'il contient.

→ Voir **Attaque informatique**, **Exploit kit**, **Intrusion informatique**, **Tutoriel** et **Zero Day**.

Fouille de données

La fouille de données, mieux connue sous le terme anglais de *datamining*, est une technique d'extraction de connaissances valides et exploitables à partir de grands volumes de données brutes provenant de sources et de bases diverses, permettant de dégager un savoir opérationnel et exploitable, notamment à des fins de marketing.

→ Voir **Big data**, **Courtier en données**, **Donnée**, **Donnée personnelle**, **Données publiques** et **Doxxing**.

Fournisseur d'accès Internet

Un fournisseur d'accès Internet (FAI), est un organisme qui offre une connexion à Internet. La traduction anglaise « *Internet Access Provider* » (*IAP*) est utilisée indifféremment. Les termes « fournisseur de services Internet » (FSI) ou « *Internet Service Provider* » (*ISP*) sont aussi utilisés à tort comme synonymes.

→ Voir **Fournisseur de services Internet**.

Fournisseur de services Internet

Un fournisseur de services Internet (FSI) est un organisme qui offre des services sur Internet ou permet l'accès et l'utilisation d'Internet. Les fournisseurs d'accès à Internet (FAI) sont des FSI particuliers.

→ Voir **Courrier électronique**, **Fournisseur d'accès Internet**, **Moteur de recherche** et **Navigateur Internet**.

Full disclosure

Le mouvement *full disclosure*, au contraire du mouvement antisec, regroupe des hackers et des spécialistes de la sécurité informatique favorables à la transparence en matière de problèmes de sécurité.

→ Voir **Antisec**, **Faille** et **Zero Day**.

Fullz

Cet anglicisme est dérivé du terme anglais « *full* », qui signifie « complet ». Il s'agit de données personnelles vendues ou achetées sous la forme d'une identité dite « complète », incluant au moins le nom complet, l'adresse, les numéros de téléphone, adresses mail (mots de passe inclus), numéros d'immatriculation sociale, et possiblement les informations bancaires ainsi que de crédit.

→ Voir **Donnée personnelle** et **Usurpation d'identité**.

- G -

Gamer

Cet anglicisme désigne une personne qui passe un certain temps à jouer à des jeux vidéo, sans pour autant en avoir nécessairement fait sa profession.

→ Voir **Administrateur**, **Avatar** et **MMORPG**.

Gestion des risques

La gestion des risques, ou le *management* des risques, est une discipline qui s'attache à identifier, évaluer et prioriser les risques relatifs aux activités d'une organisation, quelles que soient la nature ou l'origine de ces risques, pour les traiter méthodiquement de manière coordonnée et économique, de manière à réduire et contrôler la probabilité des événements redoutés afin de réduire leur impact éventuel.

Dans le contexte informatique, la gestion des risques est surtout illustrée par l'attitude du *National Institute of Standards and Technology* (*NIST*) américain suite à l'*executive order 13636* publié par le Président Obama en février 2013. Le *NIST* propose de répondre aux menaces informatiques par le changement des structures organisationnelles.

Glitch

Ce terme anglais est généralement traduit comme « pépin technique ». Il couvre tous les problèmes matériels, tous les problèmes de hardware.

Voir **Bug**, **Hardware** et **Software**.

Green hat

Ni *black hat*, ni *white hat*, ces *hackers* manifestent un respect variable pour les lois et les impératifs moraux. Ce sont basiquement des mercenaires, qui se définissent par le vert, couleur du dollar américain.

→ Voir **Black hat** et **White hat**.

Grey hat

Les *grey hats* diffèrent des *white hats* en ce qu'ils pénètrent parfois dans des systèmes sans en avoir reçu l'autorisation, acte techniquement illégal. Ils se distinguent des *black hats* en

ce que leur objectif n'est ni de causer des nuisances ni de parvenir à leurs fins mercenaires mais de se distinguer par l'accomplissement d'*exploits* informatiques. Cette catégorie recouvre le large panel de personnes se situant entre le *black hat* et le *white hat*.

→ Voir **Black hat** et **White hat**.

- H -

Hacker

Les programmeurs, qui se considèrent comme des *hackers* eux-mêmes, considèrent qu'il s'agit d'un spécialiste de la programmation, du système ou du réseau, ou encore de toute personne analysant un système inconnu de façon méthodique, et souvent empirique. L'objectif est de le connaître assez pour le dépanner, voire l'améliorer.

Le commun des mortels entend plutôt, par ce terme, celui de *black hat*.

→ Voir **Black hat**.

Hacktiviste

Les programmateurs sollicitent là encore l'utilisation du terme *cracktivistes*. Ces *hackers*, pour défendre une cause aux contours souvent flous, n'hésitent pas à transgresser la loi et attaquer des organisations pour les paralyser et obtenir des informations. L'utilisation de l'expression « désobéissance informatique » comme synonyme soulève de nombreuses protestations.

Hardware

Ce terme anglais signifie littéralement « quincaillerie ». Il désigne le matériel informatique dans son aspect matériel.

→ Voir **Software**.

Hébergeur bulletproof

Il s'agit d'un hébergeur offrant au moins les services d'hébergement classiques, en plus d'une complaisance plus ou moins grande sur l'identité des clients, les moyens de paiement, l'utilisation du service et surtout son contenu.

→ Voir **Hébergeur Internet**.

Hébergeur Internet

C'est une entité mettant à disposition des internautes des sites Internet conçus et gérés par d'autres. Il maintient des ordinateurs allumés et connectés en continu, par exemple des serveurs, à jour et fonctionnels.

→ Voir **Hébergeur bulletproof** et **Serveur Internet**.

- I -

ICANN

L'*Internet Corporation for Assigned Names and Numbers* (en Français, la « Société pour l'attribution des noms de domaine et des numéros sur Internet ») est une société de droit californien à but non lucratif ayant pour principales missions d'administrer les ressources numériques d'Internet, telles que l'adressage *IP* et les noms de domaines, ainsi que de coordonner les acteurs techniques.

→ Voir **IP**, **Nom de domaine** et **URL**.

Identité

L'identité est l'ensemble des données permettant d'établir qu'une personne est bien celle qu'elle se dit ou dont l'on présume qu'elle l'est.

Ingénierie sociale

Traduction littérale de l'Anglais, ce terme désigne une approche utilisée couramment par les *hackers* pour obtenir des informations de façon déloyale, en exploitant les failles humaines et sociales d'une structure cible pour atteindre un système informatique. Les spécialistes de l'ingénierie sociale sont similaires aux escrocs classiques en ce sens qu'ils utilisent leurs connaissances, leur charisme, des stratagèmes ou leur culot pour parvenir à leurs fins. Ils en diffèrent car ils évitent tout contact physique, ce sont des professionnels du coup de fil ou du mail.

Intrusion informatique

L'intrusion est le fait, pour une personne ou un objet, d'accéder à un document ou à un système informatique défini, que ce soit un réseau, un programme ou une machine, où sa présence n'est pas souhaitée.

Investigation financière

L'investigation financière est l'analyse d'éléments matériels économiques et financiers à tous les stades des enquêtes dans une démarche forensique de façon à recueillir des preuves des infractions et à identifier leurs auteurs pour identifier et saisir les produits du crime.

IP

Ce sigle vient de l'anglais « *internet protocol* ». Toute communication sur Internet est basée sur ce protocole, qui permet aux ordinateurs de communiquer entre eux. Il les distingue entre eux par des adresses numériques. Ce « numéro IP » permet d'identifier une machine connectée sur le réseau Internet. Ensuite, le protocole Internet tronçonne la communication en paquets qui comportent chacun une adresse de source et une adresse de destination.

→ Voir **IP Spoofing** et **Nom de domaine**.

IP spoofing

Il s'agit d'une mystification perpétrée sur un réseau, consistant à apparaître sous une adresse IP qui n'est pas la sienne.

→ Voir **IP**.

IRL

Ce sigle anglais signifie « *In Real Life* », soit littéralement « dans la vie réelle ». Les *gamers* et les *hackers* utilisent cet acronyme pour qualifier toute action réalisée dans le monde physique et matériel, par opposition avec les mondes virtuels où ils évoluent aussi. Ils peuvent aussi parler de « monde réel » ou d'*outernet*.

→ Voir **Cyberespace** et **Gamer**.

- J -

Jailbreak

Ce terme, qui signifie littéralement « évasion de prison », désigne le débridage de matériel ou d'un logiciel par le contournement d'une *MTP*. L'action, le *jailbreaking*, va nécessiter une modification du matériel ou du logiciel, ce qui peut être illégal ou simplement contraire au contrat de vente.

→ Voir **MTP**.

- L -

Logiciel espion

La traduction anglaise de ce terme, « *spyware* », est utilisée comme synonyme. Dans les deux cas, il s'agit d'un logiciel dont l'objectif est de collecter et de transmettre à des tiers des informations à l'insu des propriétaires et des utilisateurs du matériel ou des réseaux où ce logiciel malveillant est installé.

- M -

Malware

Ce terme anglais peut se traduire par « logiciel malveillant », ce qui recouvre tout programme développé dans le but de nuire à un système informatique ou à un réseau, ou par leur biais. Ce logiciel, implanté dans un ordinateur à l'insu de son propriétaire, peut être un virus, un ver ou un « cheval de Troie », trois types de codes malveillants.

→ Voir **Cheval de Troie**, **Ver** et **Virus informatique**.

MMORPG

Ce sigle, utilisé indifféremment avec celui de « *MMO* », désigne les « *massively multiplayer online role playing game* » – soit, en Français, « jeu de rôle en ligne rassemblant beaucoup de joueurs ». Ces jeux se jouent en ligne, chaque joueur incarne un personnage, son avatar, qu'il fait évoluer dans un monde virtuel généralement persistant (ne cessant jamais d'exister, évoluant même en l'absence du joueur). À la différence des jeux vidéo classiques, la plupart des personnages sont d'autres joueurs.

→ Voir **Administrateur**, **Avatar** et **Gamer**.

Money remittance

Il s'agit d'une prestation de service consistant pour un intermédiaire à transférer via un système de transfert international de fonds, sur les instructions de son client, une somme d'argent versée préalablement en espèces à un bénéficiaire désigné par le client. En général, ce type de service est proposé par les bureaux de change, bien qu'il se développe aussi aujourd'hui dans d'autres secteurs d'activités.

→ Voir **Smurfer**.

Moteur de recherche

Un moteur de recherche est un service indexant tous les sites Internet et qui, à une requête, va faire correspondre les pages Internet les plus pertinentes.

→ Voir **Déréférencement** et **Fournisseur de services Internet**.

MTP

Il s'agit de l'acronyme de « mesure technique de protection », mesure destinée à contrer le vol de contenus multimédias, généralement par la création d'une incompatibilité entre contenants et lecteurs. Par exemple, dans l'arrêt *Mulholland Drive*, il s'agissait d'un empêchement technique à la copie d'un DVD. La Cour de cassation a affirmé qu'il n'y avait pas de droit à la copie privée, mais seulement une possible exception légale au principe prohibant toute reproduction intégrale.[376]

→ Voir **Jailbreak**.

- N -

Navigateur Internet

Un navigateur Internet, ou navigateur web, est un logiciel informatique qui permet de consulter le *world wide web*, d'en visualiser les pages et d'utiliser les liens hypertextuels pour naviguer de l'une à l'autre.

→ Voir **Fournisseur de services Internet**.

Nom de domaine

Un nom de domaine (NDD) est l'adresse nominative d'un site web, d'un ensemble de sites web ou de services. Chacun est unique. Ils sont composés d'un corps et d'une extension, éventuellement précédé d'un sous-domaine. Le nom de domaine de l'université de Strasbourg, par exemple, « unistra.fr » est composé d'un corps, « unistra » et d'une extension, « fr ». Cette désignation est plus facile à utiliser que l'adresse IP qui correspond au domaine, « 130.79.201.195 ».

Les noms de domaine sont regroupés dans le *Domain Name System* (*DNS*), une base de données gérée par l'ICANN depuis 1998. L'extension va indiquer quel organisme particulier est responsable de sa gestion : le « .com » est la responsabilité de l'ICANN, le

376 Cass. Civ. 1re, 19 juin 2008, *Universal Pictures vidéo France c/ M. Stéphane X.*

« .fr » de celle de l'Association française pour le nommage Internet en coopération (AFNIC). Ce sont les registraires de noms de domaine (« *registrar* », en Anglais), des sociétés ou des associations, qui gèrent la réservation.

→ Voir **ICANN**, **IP** et **URL**.

NS

C'est l'acronyme de *Nation State*, qui désigne les *hackers* des agences de renseignements et les agents de cyberguerre, employés par les gouvernements et leurs déclinaisons.

- O -

Ouverture des données

Derrière l'expression anglais *open data*, se cachent deux concepts.

D'abord, il y a celui d'ouverture des données, un principe selon lequel les données publiques doivent être disponibles pour accès et réutilisation par les citoyens et les entreprises. Ces données sont alors dites « données ouvertes ».

La donnée ouverte est l'autre face de l'*open data*. Elle est toute donnée publiée selon une démarche qui implique qu'elle respecte dix critères garantissant leur libre accès et réutilisation par tous : elle doit être complète, primaire, opportune, accessible, exploitable, non-discriminatoire, non-propriétaire, libre de droits, permanente et gratuite. Elle peut être d'origine privée ou publique.

À terme, l'objectif de ce courant est la suppression de toute restriction de l'exploitation et de la reproduction des licences.

→ Voir **Donnée**, **Données personnelles** et **Données publiques**.

- P -

Pair à pair

Ce terme vient de l'anglais « *peer to peer* » et désigne à l'origine une technologie permettant l'échange de données entre ordinateurs reliés à Internet, chacun étant un serveur. Ce réseau peut être décentralisé, la connexion se faisant directement entre eux, ou centralisé autour d'un serveur intermédiaire. De telles montages peuvent servir au partage de fichiers, au calcul distribué ou à la communication.

Le sigle « *P2P* » recouvre désormais l'intégralité du modèle économique dont la technologie a favorisé l'apparition. Son principe de base est la mise en commun à une vaste échelle de données ou de capacités, ce qui permet de réduire leurs coûts.

→ Voir **Serveur Internet**.

Pare-feu

La traduction anglaise de ce terme, « *firewall* », est plus utilisée. Le pare-feu est un équipement, généralement un logiciel, qui protège un ou plusieurs ordinateurs connectés à un réseau, par exemple Internet. Il doit réaliser un filtrage entrant, repoussant les attaques externes, et sortant, empêchant les extractions illégitimes.

→ Voir **Attaque informatique** et **Intrusion informatique**.

Pénétration sur Internet

Il s'agit de la corrélation entre le nombre d'internautes dans chaque pays et sa population. Elle est exprimée sous la forme du pourcentage de la population qui a accès à Internet.

Pharming

Il s'agit d'un mode opératoire très élaboré et transparent, consistant à contraindre un serveur DNS à rediriger une requête d'accès, non pas sur l'adresse IP correspondant à l'URL, mais sur un faux site, ce détournement de connexion visant à capturer des informations confidentielles.

→ Voir **IP**, **Nom de domaine**, **Serveur Internet** et **URL**.

Phishing

Également appelé « hameçonnage » ou « filoutage », c'est une technique de fraude reposant sur l'ingénierie sociale. Il s'agit d'obtenir les données personnelles ou bancaires d'une victime en se faisant passer pour un tiers de confiance. Le *phishing* peut employer différents canaux de diffusion (sites Internet, mails, SMS, téléphone, etc).

→ Voir **Courrier électronique**, **Ingénierie sociale** et **Spam**.

Phreakers

Le *phreaker* est un type très particulier de *hacker*, qui exploite et pirate le système téléphonique. C'est un jeu de mot entre les mots *phone* et *freak*, qui signifient respectivement « téléphone » et « monstre ». Aujourd'hui, le *phreaking* est surtout un hobby mais ses pratiquants étaient les précurseurs des *hackers* tels que nous les

connaissons.

Piratage de sites

Il s'agit de la pénétration sans accord préalable dans un système, avec éventuellement duplication ou diffusion des données ou programmes qu'il contient, alors que leurs ayant-droits l'interdisent.

→ Voir **Black hat**.

Proxy

Il s'agit d'une machine connectée à Internet et servant d'intermédiaire à une autre pour y accéder. Généralement, il s'agira d'un serveur informatique dont la fonction est de relayer des requêtes entre un ordinateur et un autre serveur. Il peut jouer le rôle de pare-feu, bloquant les accès et sorties non autorisées, ou assurer la sécurité des ordinateurs locaux, leur filtrage et leur anonymat.

→ Voir **Pare-feu**, **Serveur Internet** et **TOR**.

- R -

Ransomwares

Ce terme anglais accole les termes *ransom*, signifiant « rançon », et *ware*, qui désigne le logiciel. Il est parfois francisé en « rançongiciel ». Ces logiciels infectent une machine puis procèdent discrètement à des opérations grâce auxquelles le pirate pourra exiger une rançon, contre le déblocage de la machine, le déchiffrage des fichiers ou la non divulgation de leur contenu.

RAT

Ce peut être l'acronyme de « *remote administration tool* », terme qui désigne des programmes plutôt bénins, permettant l'assistance ou le dépannage de systèmes, ou « *remote access trojan* », terme qui désigne une forme particulière de chevaux de Troie. Les deux sont des outils d'administration à distance, c'est-à-dire des logiciels permettant de modifier la configuration d'une machine à travers un réseau.

→ Voir **Cheval de Troie** et **Malware**.

Rétro-ingénierie

Il s'agit de l'activité consistant à étudier un produit pour déterminer son fonctionnement

interne ou sa méthode de fabrication. L'objectif sera de comprendre son fonctionnement à des fins de bonne utilisation ou de perfectionnement, de copier le produit ou ses fonctionnalités sans accès à ses plans ou méthodes de fabrications ou d'analyser le produit d'un concurrent à des fins de renseignements.

On parle aussi d'« ingénierie inverse » ou « d'ingénierie inversée ».

Rippers

Ce terme anglais, qui dérive du verbe « *rip* », se traduisant par « déchirer », désigne un cybercriminel qui se fait passer pour un vendeur légitime sur un site de *black market* ou qui crée de faux sites de ce genre pour récupérer le montant de transactions illégales sans offrir de réelles contreparties.

→ Voir **Darknets**.

Robot d'indexation

Le robot d'indexation, mieux connu sous les anglicismes « *crawler* » ou « *spider* », est un robot logiciel qui explore automatiquement des sites et contenus Internet. Ils les indexent et analysent les contenus explorés en partant des résultats d'un moteur de recherche, à partir d'une liste, par soumission ou en suivant tous les liens rencontrés. Les contenus parcourus et l'ampleur de l'exploration dépendront de la nature du robot et de ses objectifs. Souvent, il s'agira de recueillir des ressources. Les spammeurs les utilisent ainsi pour recueillir des adresses électroniques auxquelles envoyer des pourriels.

→ Voir **Spam**.

Rootkit

Un *rootkit* est un logiciel ou un ensemble de logiciels, dont le but est d'obtenir et de pérenniser un accès furtif, généralement non autorisé, à un ordinateur. Parfois, l'accès n'est pas furtif mais le logiciel est impossible à désinstaller.

Ils peuvent installer des logiciels malveillants sur les machines ou s'assurer du respect des conditions d'utilisation des produits qu'ils accompagnent.

- S -

Script kiddies

Ce terme anglais signifie littéralement « gamins qui utilisent des scripts ». Sans grande

compétence, ils se livrent au piratage informatique par forfanterie et utilisent souvent les programmes d'autres *hackers*. Le reste de leur communauté ne les considère pas réellement comme des *hackers*, alors qu'eux s'incluent dans ce nombre. On oppose aux *script kiddies* les codeurs, pirates capables de créer leurs propres outils d'intrusion, équivalents illégaux, formellement éduqués ou non, du programmeur.

→ Voir **Codeurs**, **Exploit kit**, **Hacker** et **Tutoriel**.

Serveur Internet

Un serveur Internet est un ordinateur équipé d'un logiciel qui lui permet d'utiliser le protocole de communication employé sur le *world wide web* et qui est utilisé pour publier des sites sur Internet ou un intranet. En sus, il peut offrir d'autres services comme l'envoi de mails, le streaming, etc mais sa fonction principale est le stockage et la publication des pages Internet.

→ Voir **Hébergeur Internet**.

Sextorsion

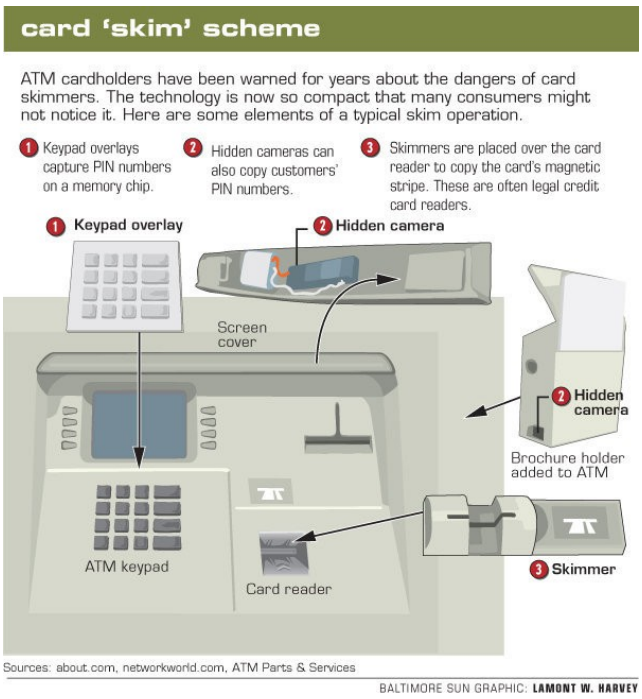
Un « agent » travaillant pour une organisation criminelle recrute des cibles sur Internet, généralement par le biais de réseaux sociaux, de sites de rencontres, de sites de dialogue vidéo en ligne ou de sites pornographiques. Il gagne la confiance de ses victimes afin de les convaincre de le laisser enregistrer des images d'elles en train de se livrer à des activités sexuelles.

Il les menace ensuite de publier ces images sur Internet ou de les diffuser auprès des amis de la victime si celle-ci refuse de lui verser une certaine somme. Il peut aussi pratiquer d'autres techniques d'extorsion, par exemple en se faisant passer pour les forces de l'ordre.

Skimmer

Dans le contexte de la fraude aux distributeurs de billets, un *card skimmer*, représenté ci-contre, est un dispositif double permettant d'enregistrer en vidéo le code saisi par l'usager et de copier la piste magnétique de la carte insérée. On parle aussi d'« écumoire » ou de « dispositif de copie de carte », de « faux dispositif de retrait d'argent » ou encore de « distributeur modifié de façon frauduleuse ».

Cette technique est bien distincte de celle dite du « collet marseillais », où le distributeur a été modifié pour retenir la carte de crédit et où c'est un complice humain qui relève le code de la carte bleue pendant que la victime le tape.



→ Voir **Carding** et **Hardware**.

Smurfer

Ce terme vient du verbe anglais « *smurf* », qui désigne une certaine architecture des transactions financières, qui consiste à les diviser en plusieurs petites opérations pour éviter d'attirer l'attention des autorités. Le mot « *smurfer* » désigne tout individu dont l'activité sert à assurer l'anonymat d'un criminel, soit alors qu'il se fournit en matériaux, soit alors qu'il récupère ses gains illicites. Dans le milieu des stupéfiants, les forces de l'ordre appellent ainsi l'individu, en général un drogué, qui pourvoit son *dealer* en matériaux de base. Dans la cybercriminalité, c'est la personne qui transfère des fonds acquis illégalement en personne, via un service postal ou électronique, de la part d'un tiers. Il est payé pour ses services, généralement sous la forme d'une commission.

Une variante du *smurfer* est la *money mule*. Elle est souvent une victime elle-même, appâtée par une offre d'emploi d'apparence licite et totalement inconsciente du fait que l'argent transféré est le produit d'une activité criminelle. Elle utilise principalement des services de transfert instantané de fonds anonymisant les transactions, tels que *Ukash* ou *Western Union*. Elle protège l'identité et la localisation du criminel. Elle encourt des risques juridiques.

Une autre est la « flèche ». Dans le cas de réseaux très localisés se livrant à une activité cybercriminalité, la flèche est un membre du réseau, généralement de bas étage, qui va collecter les gains frauduleux et les transférer suivant un processus assurant leur opacité à son organisation.

Une autre est le *drop*, ressortissant d'un pays ne réprimant pas les délits numériques

(Indonésie, Malaisie, Bolivie, etc). Il transfère les gains illicites sur son compte en banque, en garde autour de 50% et rend au cybercriminel l'autre moitié de la somme, blanchie.

→ Voir **Money remittance**.

Snowshoe spamming

Ce terme vient de la façon dont une raquette (en Anglais, « *snowshoe* ») répartit le poids du marcheur. Il désigne une technique de *spamming* qui répartit l'expédition des *spams* entre de nombreuses adresses *IP* et domaines afin de les protéger d'un éventuel listage.

→ Voir **IP, IP Spoofing**, **Nom de domaine** et **Spam.**

Software

Ce terme anglais désigne un logiciel. Il a été créé par opposition au *hardware*. Il recouvre l'élément immatériel, le code.

→ Voir **Hardware**.

Spam

Le *spam* est un courrier électronique qui se caractérise par un envoi massif et souvent répété à des personnes avec lesquelles l'expéditeur n'a jamais eu de contact et dont il a récupéré les adresses électroniques de façon irrégulière. Le mot « pourriel » est utilisé comme synonyme.

Une variante du *spam* est le « *spim »,* abréviation de « *spam over instant messaging* », qui désigne une forme de *spam* diffusé par le biais des messageries instantanées. Une autre forme de *spamming* est le *SPIT*, acronyme de « *SPam over Internet Telephony* ». Il recouvre toute publicité indésirable réalisée sur les réseaux de communication Internet par la voix (téléphonique ou vidéos : *skype*, la visioconférence sur *Facebook*, etc).

Les spammeurs préfèrent être appelés « *adverts* ».

→ Voir **Antis**, **Courrier électronique**, **Robot d'indexation** et **Snowshoe spamming**.

STAD

Ce sont les initiales de « système de traitement automatisé de données ». Elles servent à désigner un ensemble composé d'une ou plusieurs unités de traitement automatisé de données, protégé ou non par un système de sécurité. Constituent de telles unités de traitement automatisé des données tous les équipements, *software* ou *hardware*, qui permettent leur acquisition, leur stockage, leur manipulation, leur contrôle, leur affichage,

leur transmission ou leur réception.

Le STAD est la condition préalable de l'intervention des infractions informatiques en France. Une définition avait donc été proposée lors des débats parlementaires autour de la loi *Godfrain*, en 1988, mais elle ne figure pas dans le texte, par souci de permettre l'adaptation des infractions aux évolutions de la technologie. En 2013, la cour de cassation a d'ailleurs eu à refuser la transmission d'une question prioritaire de constitutionnalité (QPC) sur la conformité au principe de légalité des délits et des peines d'une telle omission du législateur.[377]

→ Voir **Cybercriminalité**, **Donnée**, **Hardware** et **Software**.

- T -

TOR

C'est l'acronyme des mots anglais « *the onion router* », nom d'un réseau mondial décentralisé de routeurs organisés en couches. Il assure l'anonymat complet de ses utilisateurs, puisque ni l'internaute navigant sur un site caché ni le serveur qui héberge le service n'ont accès à l'identité l'un de l'autre. Au départ, il a été conçu par l'armée américaine mais il est passé dans le domaine public et les cyberdélinquants en sont friands.

→ Voir **Deep web**, **Proxy** et **Serveur Internet**.

Troll

En ligne, il s'agit d'un individu qui persiste à lancer et maintenir des polémiques. C'est un hommage au troll semeur de zizanie de la mythologie nordique.

Tutoriel

Ce terme vient de l'Anglais « *tutorial* » et désigne comme lui un outil pédagogique – logiciel, vidéo, document électronique ou papier – constitué d'instructions détaillées pas à pas. Ce guide d'apprentissage vise en général le domaine informatique et permet d'aider l'utilisateur novice à se former de manière autonome à l'utilisation d'un logiciel, à un langage de programmation ou à des jeux interactifs. Dans le milieu du piratage informatique, les tutoriels se monnaient en ligne.

377 Cass., crim., 10 avril 2013, n° 12-85.618 : la Cour n'a pas amené d'éléments de définition, elle a seulement considéré que les conditions de transmission, ici le caractère sérieux, n'étaient pas remplies « *dès lors que les termes de l'article 323-3 du code pénal sont suffisamment clairs et précis pour que son interprétation et sa sanction, qui entrent dans l'office du juge pénal, puissent se faire sans risque d'arbitraire.* »

→ Voir **Script kiddies**.

- U -

URL

C'est le sigle des termes anglais « *Uniform Resource Locator* », dont des synonymes seraient « adresse web » ou « adresse Internet ». Elle est l'expression de la méthode d'accès et de l'adresse de tout document publié en ligne, de toute « page », par exemple sous la forme d'un hyperlien.

Usurpation d'identité

Par « usurpation d'identité », cette étude désigne tout cas de détournement des données personnelles d'un individu à des fins illégales.

- V -

Ver

Le ver est un virus qui se propage de façon presque autonome. Ce logiciel malveillant indépendant utilise les réseaux à la recherche des failles de sécurité lui permettant de se répliquer de machine en machine. Il peut aussi se transmettre par d'autres biais. Il perturbe le fonctionnement des systèmes concernés en s'exécutant à l'insu des utilisateurs.

→ Voir **Faille**, **Malware** et **Virus informatique**.

Virus informatique

Il s'agit d'un programme informatique malveillant s'exécutant sur un système informatique pour accéder à ses ressources ou les parasiter, les compromettre ou les dégrader, et même peut-être interrompre le service fourni.

→ Voir **Cheval de Troie**, **Logiciel espion**, **Malware**, **Ransomware**, **RAT** et **Ver**.

- W -

White hat

Il s'agit d'un professionnel de la sécurité informatique qui effectue des tests d'intrusion avec l'autorisation de ses clients et conformément à la législation en vigueur pour s'assurer du

niveau de sécurité d'un système. Il arrive que des *hackers* se considèrent comme des *white hats* alors qu'ils transgressent la loi, leur but étant de prévenir les responsables des failles affectant leurs systèmes. En règle générale, la distinction entre ces deux catégories de *hackers* se basera sur trois critères : autorisation, motivation et intention.

En Français, pour désigner les *white hats*, les termes de « hacker éthique » ou de « testeur d'intrusion » pourront être utilisés.

→ Voir **Black hat** et **Faille**.

World Wide Web

Ce terme anglais recouvre l'ensemble des sites web accessibles sur Internet. Son acronyme, « WWW », figure généralement au début de toute URL.

→ Voir **Cyberespace** et **URL**.

- Z -

Zero Day

Une vulnérabilité jour zéro (ou « *zero day* ») est une vulnérabilité informatique encore inconnue ou non corrigée. La découverte d'une telle vulnérabilité par un *hacker* peut entraîner la conception d'un *exploit*, c'est-à-dire d'une technique l'exploitant mais il peut aussi la revendre ou la signaler gracieusement aux exploitants du produit informatique affecté.

→ Voir **Exploit kit** et **Faille**.

Zombies

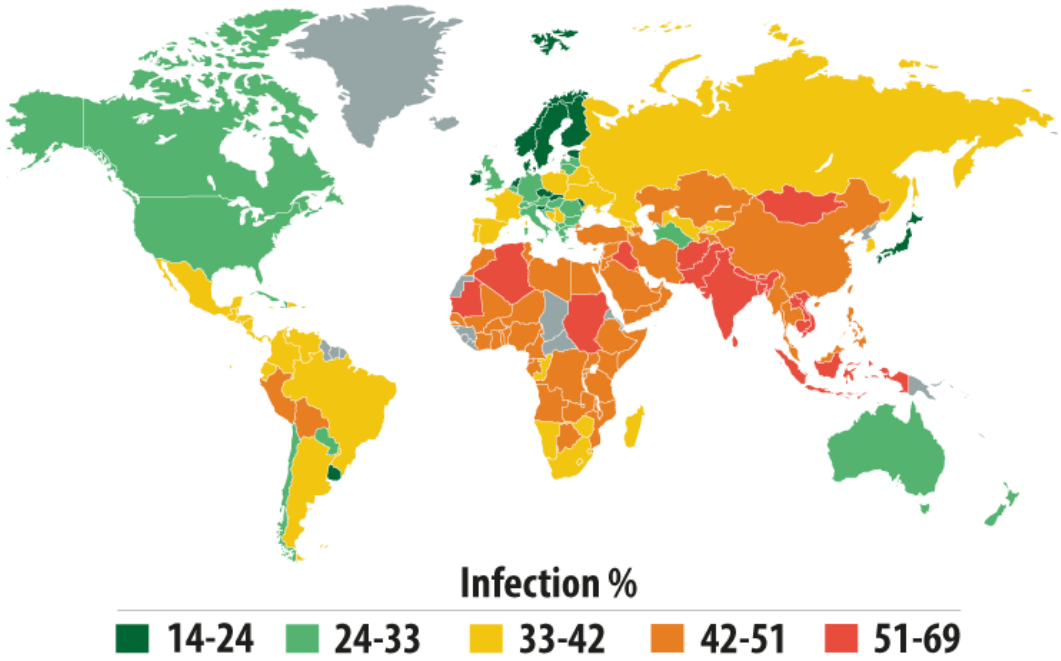
Les *bots*, abréviation de *robots*, sont usuellement les personnages d'un jeu pilotés par une machine. Dans le monde des *hackers*, il s'agit aussi d'ordinateurs pilotés à distance. Plutôt que de « *bots* », on peut parler de « machines zombies ». En général, ils sont regroupés en *botnets*, groupes de machines connectées à un réseau et pilotés par une seule entité, le *botmaster*. Ils sont ordinairement connectés à internet et utilisés à des fins malhonnêtes, par exemple pour expédier du spam ou attaquer (souvent par *DDoS*). Dans les situations entièrement légales, le terme employé est plutôt « grille ». Il arrive que les *botnets* se livrent d'épiques combats.

→ Voir **DDoS**, **RAT** et **Spam**.

Annexes

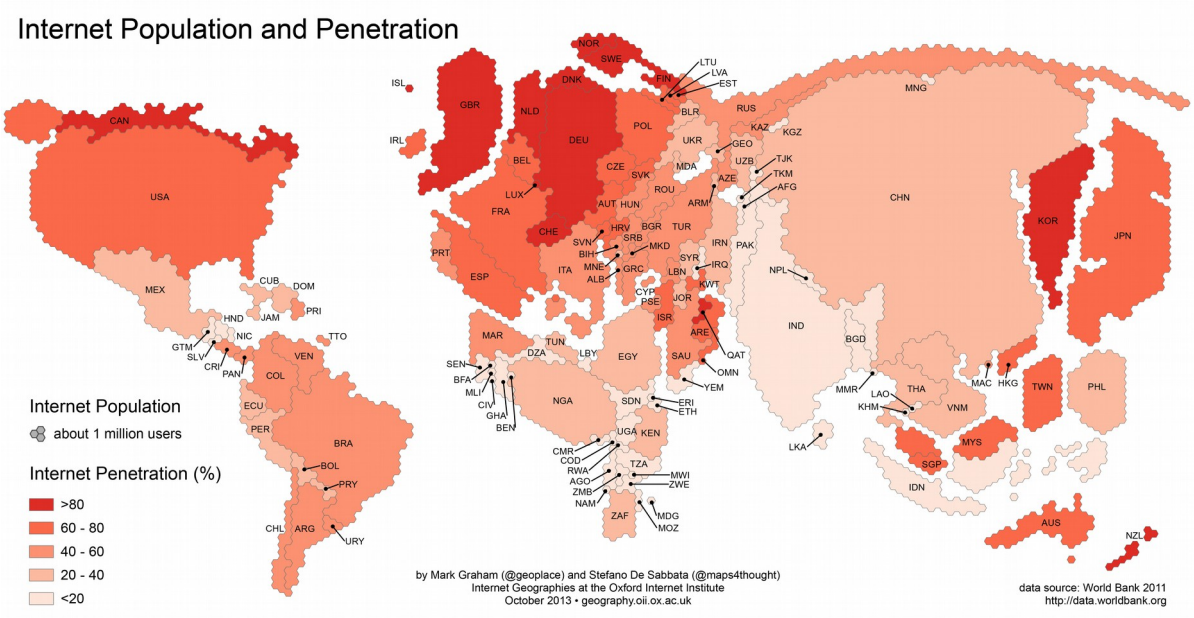
Annexe 1 : Carte des pays les plus infectés au monde

Source : Kaspersky, 2013



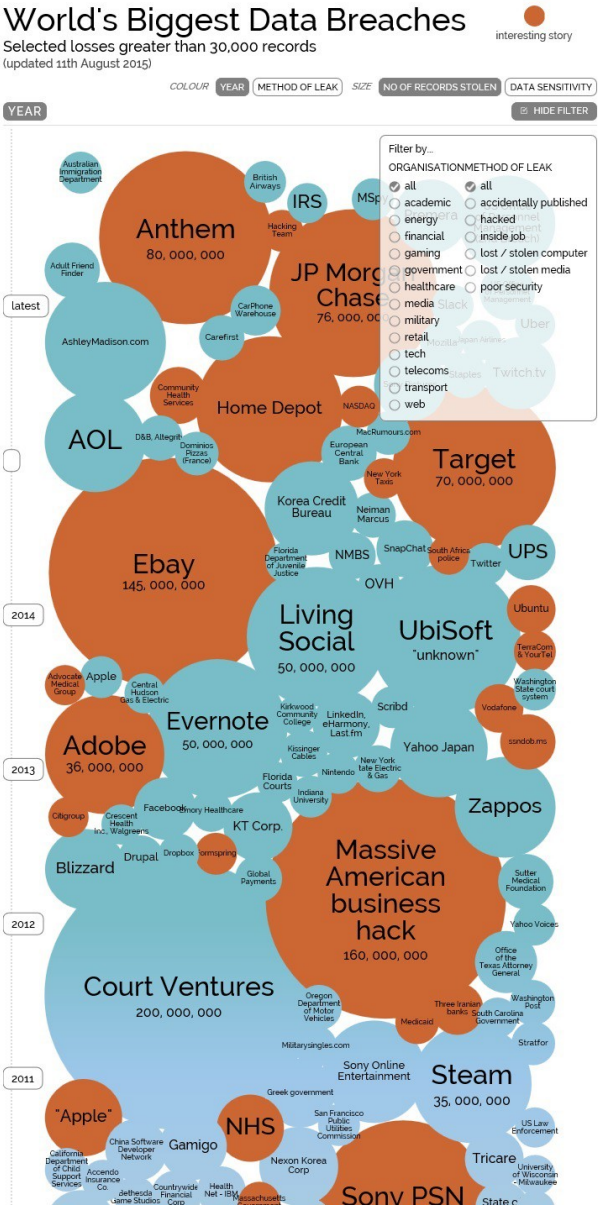
Annexe 2 : Carte de la pénétration mondiale sur Internet

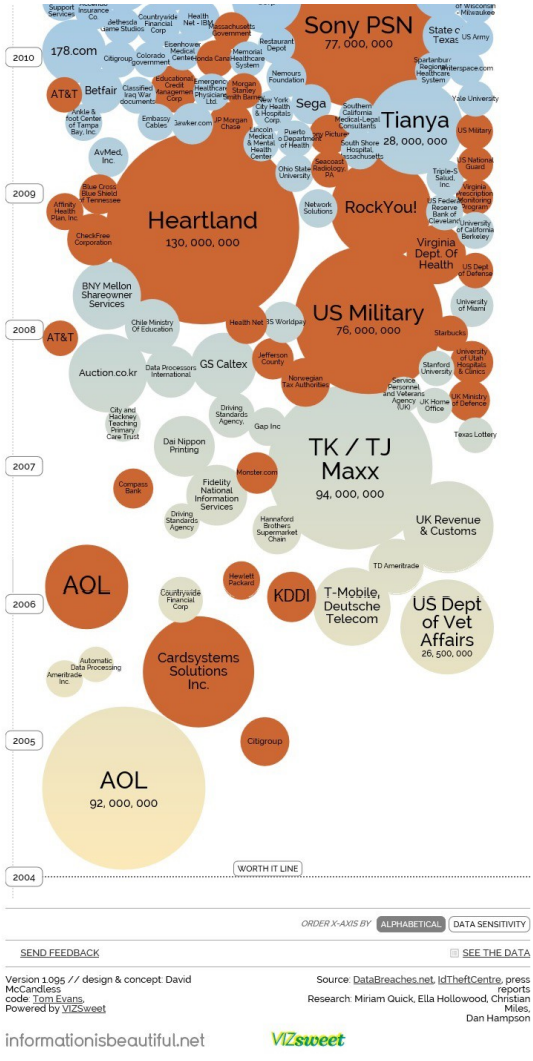
Source : Banque mondiale, 2011



Annexe 3 : Infographie des pires fuites de données (2004 -)

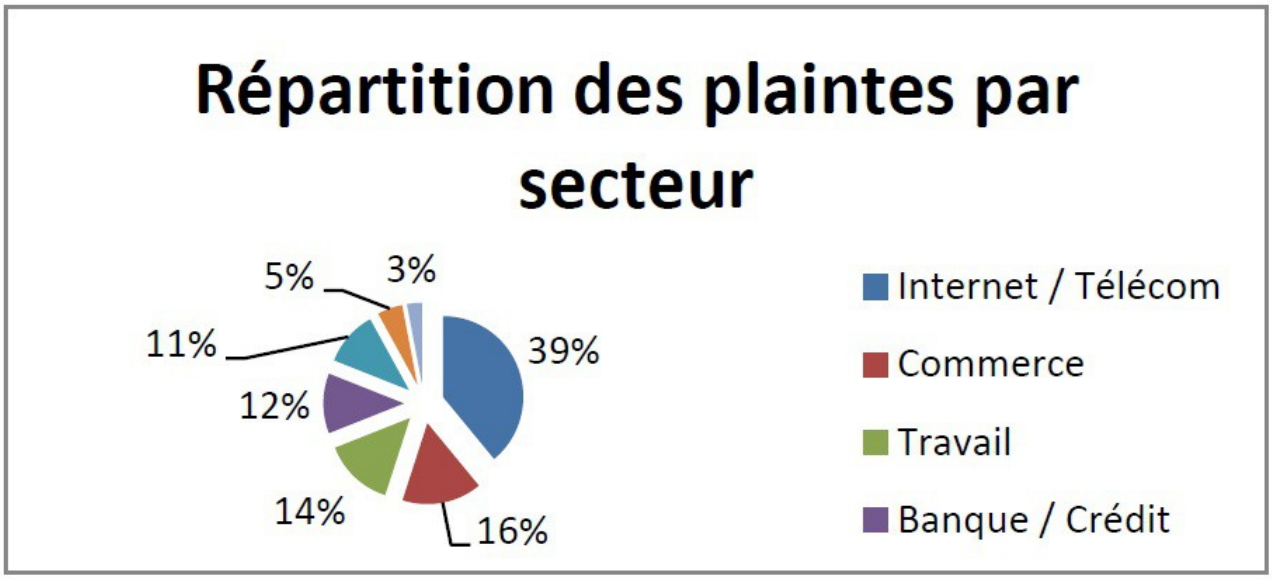
Source : [informationisbeautiful.net](), 2015





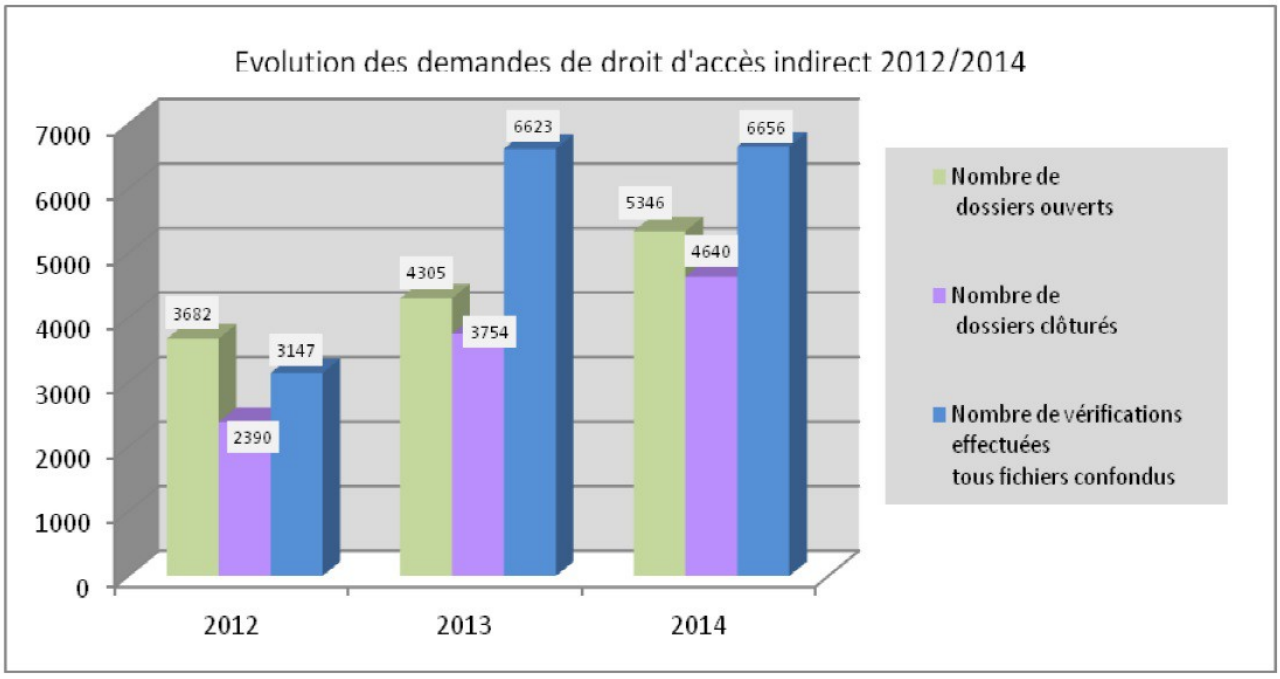
Annexe 4 : Répartition par secteur des plaintes déposées à la CNIL

Source : CNIL, 2015



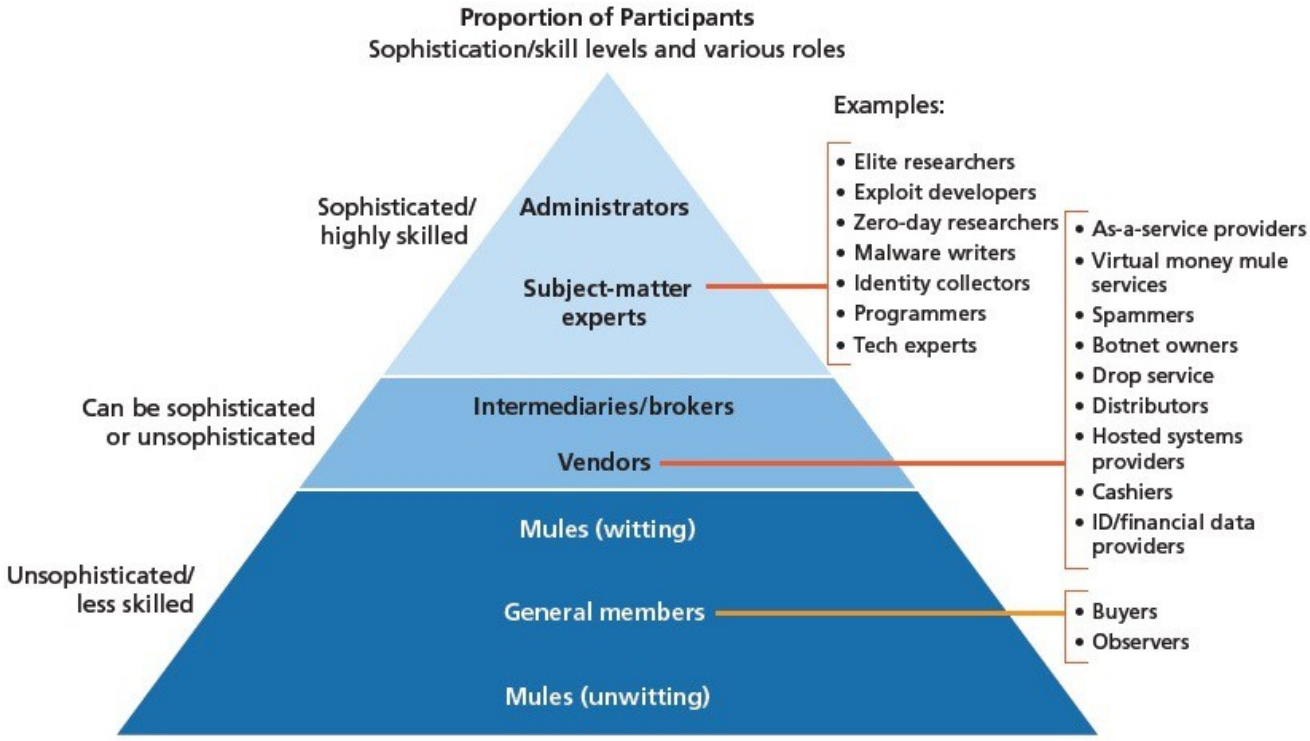
Annexe 5 : Evolution des demandes de consultation indirecte à la CNIL

Source : CNIL, 2015



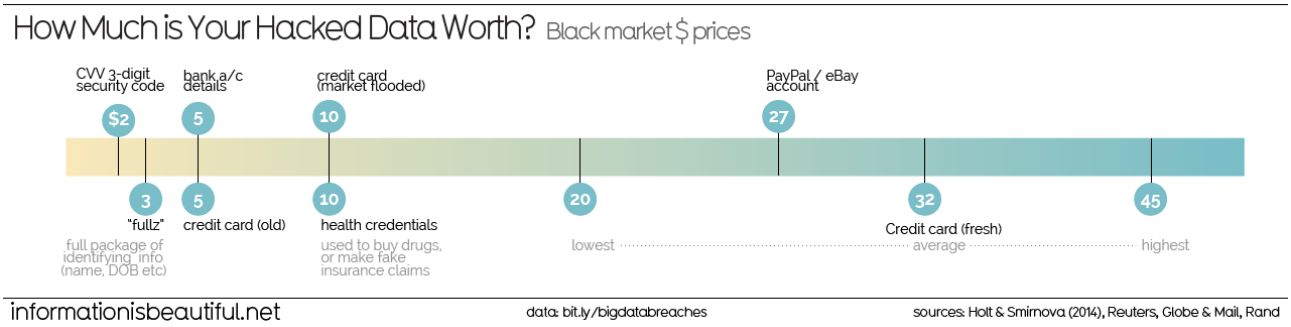
Annexe 6 : Pyramide des différents participants aux marchés noirs de la cybercriminalité

Source : RAND, 2014



Annexe 7 : Valeur des données personnelles *hackées*

Source : [informationisbeautiful.net](), 2015



Annexe 8 : Catalogue des marchés noirs de données personnelles

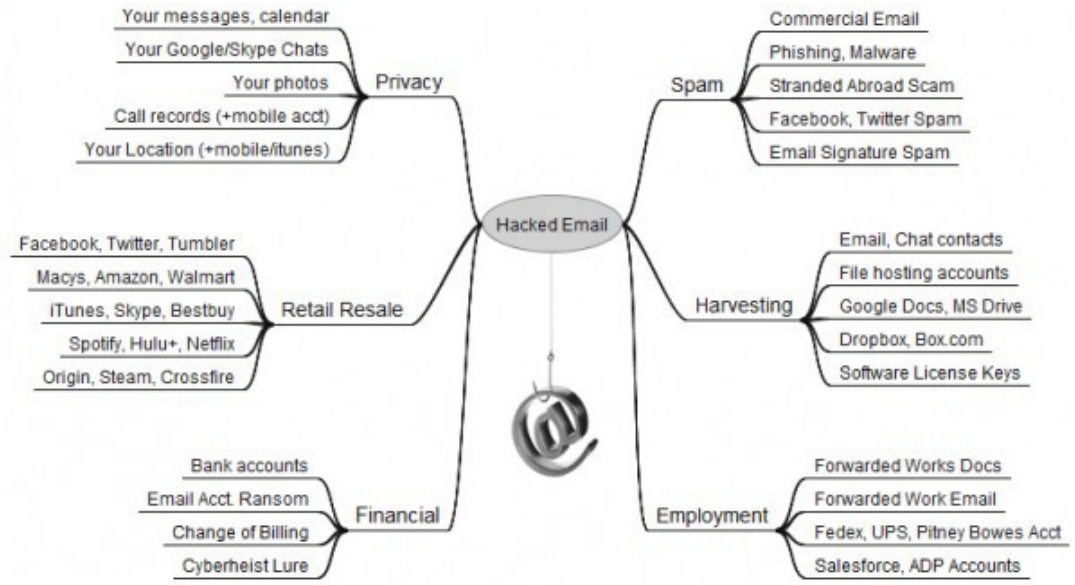
Source : Dell SecureWorks, 2014

Hacker Products and Services	Price in 2013	Price in 2014
Visa and Master Card (US)	$4	$4
American Express (US)	$7	$6
Discover Card with (US)	$8	$6
Visa and Master Card (UK, Australia and Canada)	$7 -$8	$8
American Express (UK, Australia and Canada)	$12- $13	$15(UK and Australia); $12 (CA)
Discover Card (Australia and Canada)	$12	$15(Australia); $10(CA)
Visa and Master Card (EU and Asia)	$15	$18-$20
Discover and American Express Card (EU and Asia)	$18	$18-$20
Credit Card with Track I and II Data (US)	$12	$12
Credit Card with Track I and II Data (UK, Australia and Canada)	$19-$20	$19-$20
Credit Card with Track I and II Data (EU, Asia)	$28	$28
US Fullz	$25	$30
Fullz (UK, Australia, Canada, EU, Asia)	$30-$40	$35-$45
VBV(US)	$10	$12
VBV (UK, Australia, Canada, EU, Asia)	$17-$25	$28
Premium Master Cards with Track 1 and 2 Data (Worldwide)	N/A	$35
Premium Visa Cards with Track 1 and 2 Data (Worldwide)	N/A	$23
High Quality Bank Accounts with Verified Balances of $70,000-$150,000	N/A	6% of the balance of the account
Remote Access Trojan(RAT)	$50-$250	$20-$50
Crypters	N/A	$50 -$150
Sweet Orange Exploit Kit Leasing Fees	$450 a week/$1800 a month	$450 a week/$1800 a month
Nuclear Exploit Kit Leasing Fees	N/A	$50 a day/$400 a week/$600 a month
Counterfeit Passports (Non US)	N/A	$200--$500
New Identities, plus matching utility bill	N/A	$250; matching utility bill an additional $100
Counterfeit Social Security Cards	N/A	$250-$400
Counterfeit Drivers' License	N/A	$100-$150

Hacker Products and Services	Price in 2013	Price in 2014
Hacking Tutorials	N/A	$1 each to $30 for 10 (depending on the tutorial)
Hacking Website: stealing data	$100-$300	$100 -$200
DDoS Attacks	Per Hour-$3-$5	Per Hour - $3-$5
	Per Day-$90-$100	Per Day - $60-$90
	Per Week-$400-$600	Per Week - $350-$600
Doxing	$25-$100	$25-$100
Infected Computers (US)	N/A	US (unique installs)
		1,000 - $140 - $190
		5,000 - $600 - $1000
		10,000 - $1100 - $2000
Infected Computers (UK)	N/A	UK (unique installs)
		1,000 - $100 - $120
		5,000 - $400 - $500
		10,000 - $700 - $1100
Infected Computers (Asia)	N/A	Asia (unique installs)
		1,000 - $4 - $12
		5,000/10K - N/A

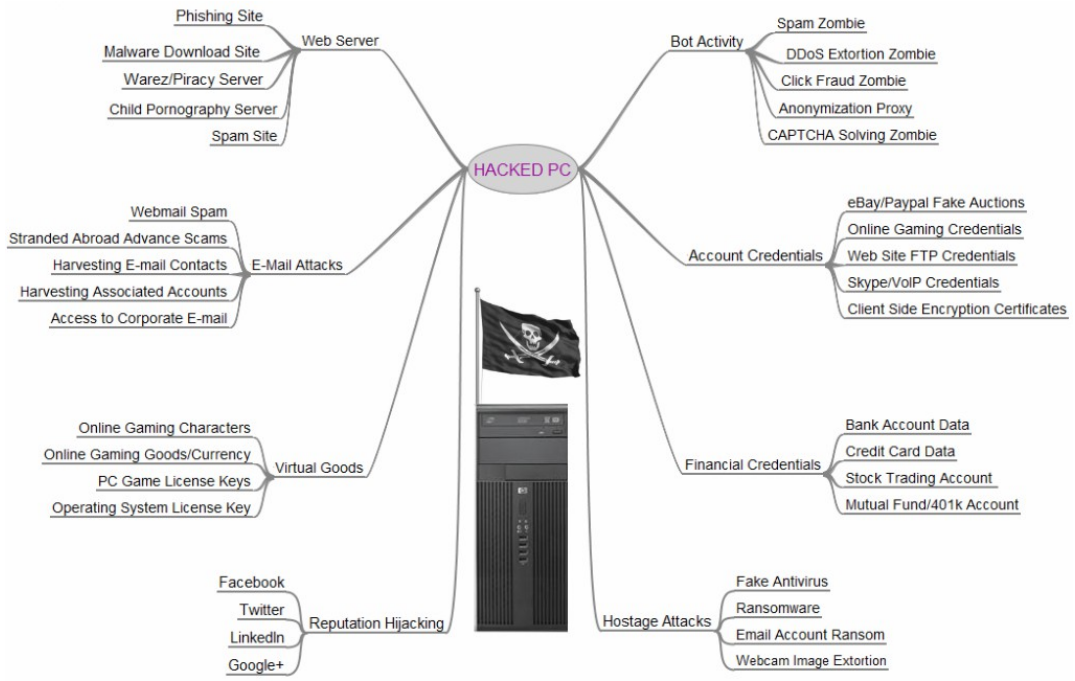
Annexe 9 : La boîte mail, objet de convoitise dans le monde du *hacking*

Source : Krebson Security, 2012



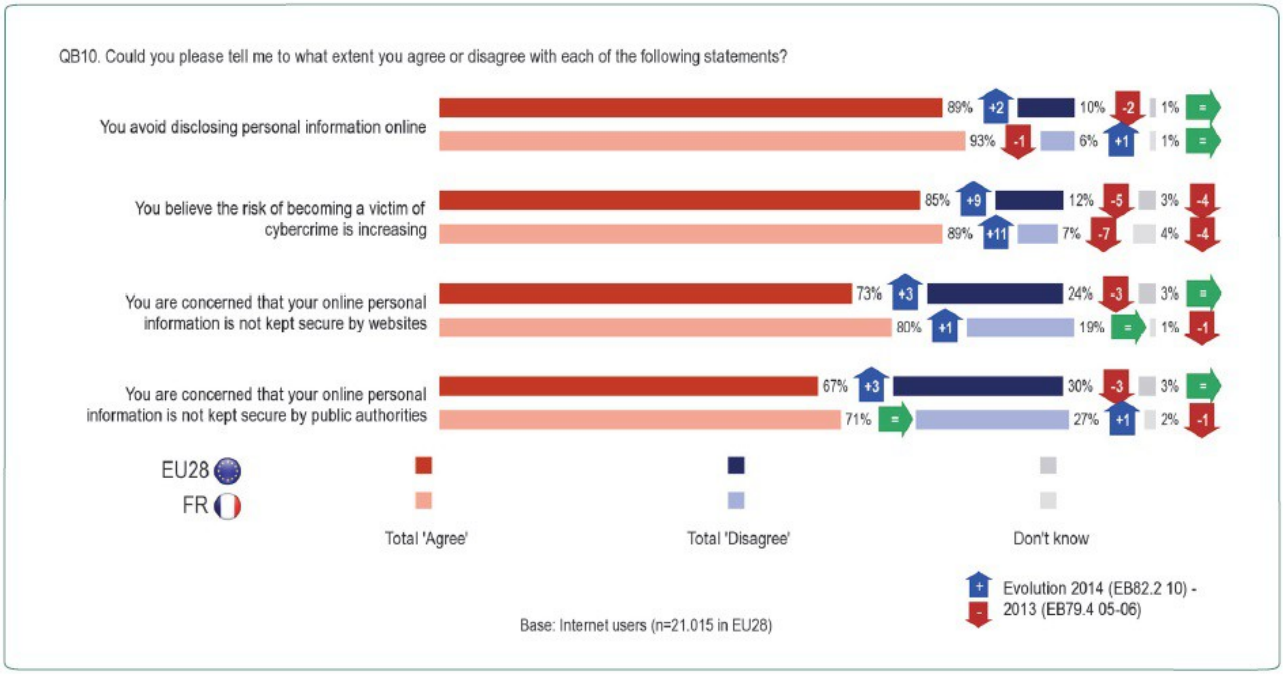
Annexe 10 : L'ordinateur zombie, un atout de prix dans la manche du *hacker*

Source : Krebson Security, 2012



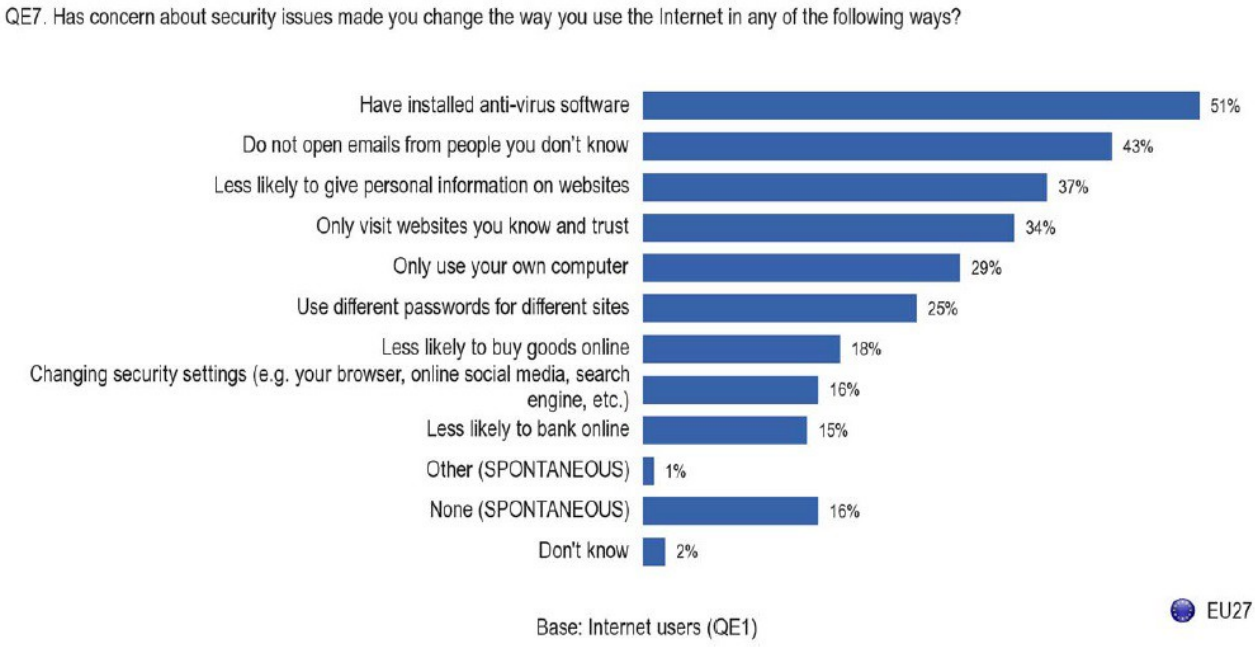
Annexe 11 : Manifestations de l'inquiétude des populations de l'UE quant à la divulgation de données personnelles

Source : Eurobaromètre, 2015



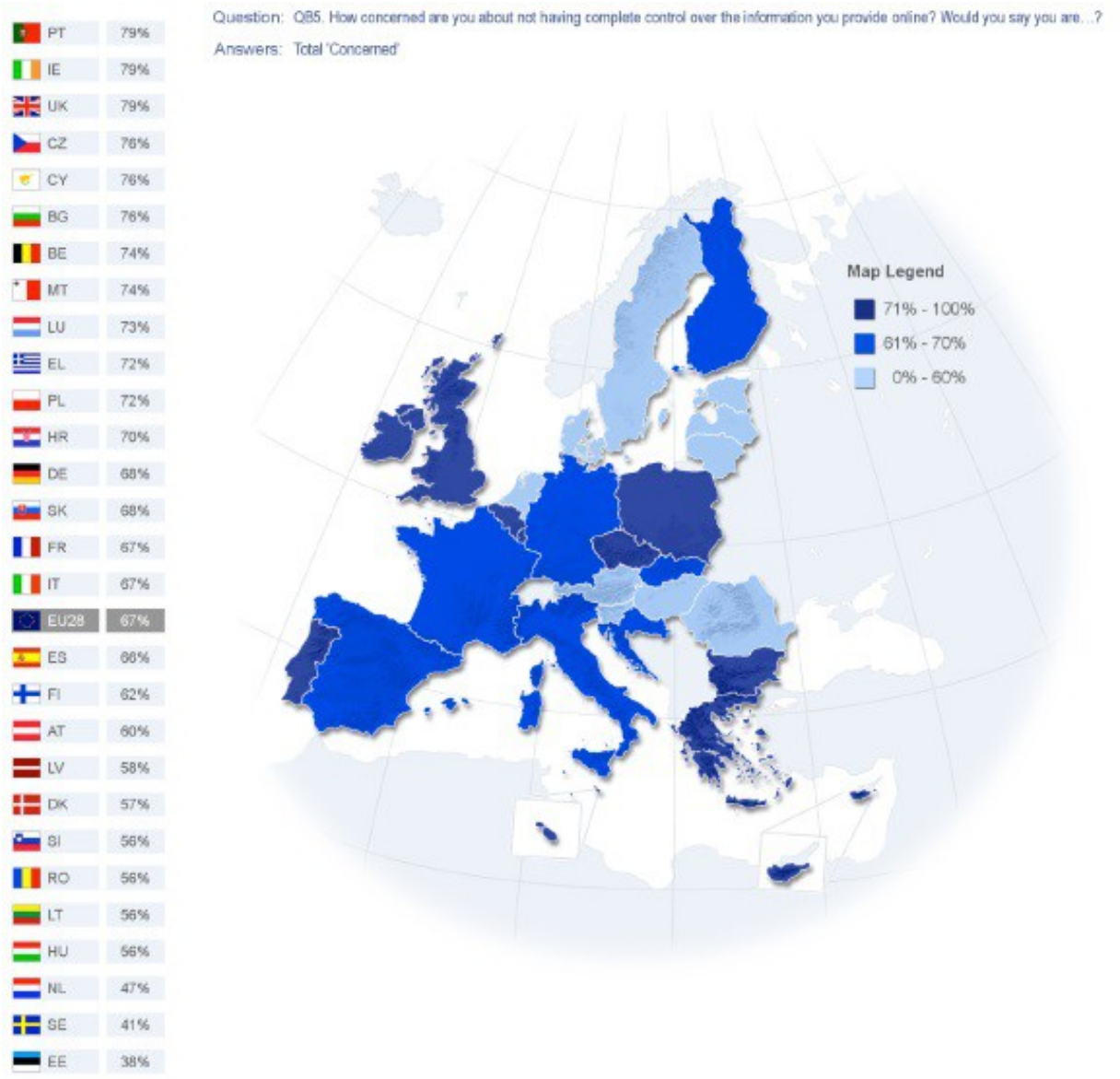
Annexe 12 : Réactions des populations de l'UE face à la crainte d'être victimes de cybermenaces

Source : Eurobaromètre, 2015



Annexe 13 : Carte de l'inquiétude des populations de l'UE quant à leur manque de contrôle sur les données personnelles qu'elles communiquent en ligne

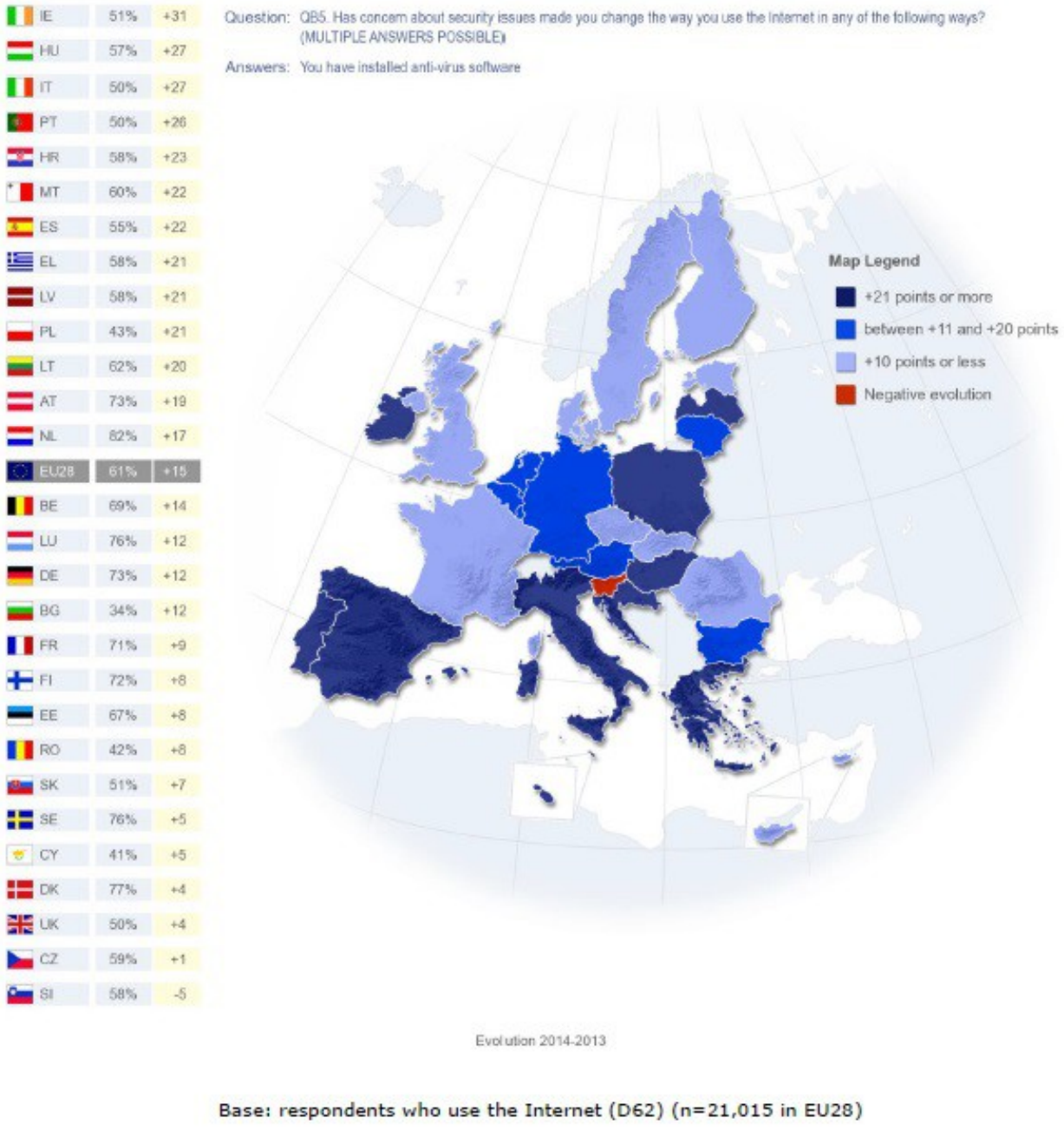
Source : Eurobaromètre, 2015



Base: Respondents who feel like they do not have complete control over the information they provide online (n=16,244 in EU28)

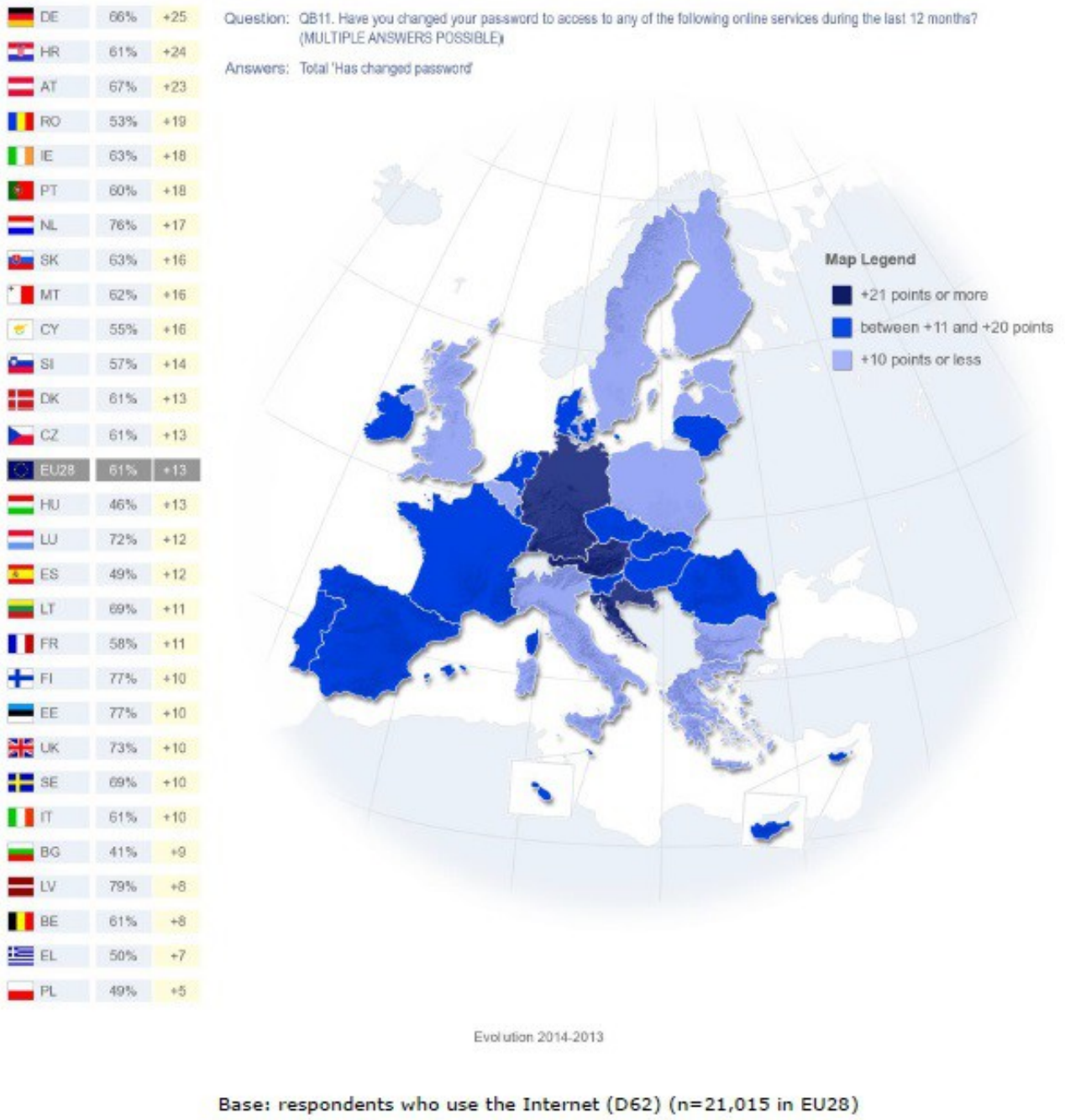
Annexe 14 : Carte : pourcentage des populations de l'UE qui ont installé un antivirus en réaction aux menaces informatiques

Source : Eurobaromètre, 2015



Annexe 15 : Carte : Européens qui changent leurs mots de passe en réaction aux menaces informatiques

Source : Eurobaromètre, 2015



Annexe 16 : Table de l'attribution de la responsabilité de la protection des données personnelles, de l'avis des populations de l'UE, par État membre

Source : Eurobaromètre, 2015

QB11T. Who do you think should make sure the personal information you provide online is collected, stored and exchanged safely? Firstly? And secondly? (MAX. 2 ANSWERS)

	Online companies – as they need to ensure they process your information safely	You – as you need to take care of your information	Public authorities – as they need to ensure that citizens' data are protected	Other (SPONTANEOUS)	You never provide personal information online (SPONTANEOUS)	Don't know
EU28	67%	66%	55%	1%	3%	2%
BE	56%	**73%**	62%	1%	3%	0%
BG	**75%**	53%	55%	0%	5%	3%
CZ	65%	**66%**	58%	0%	3%	2%
DK	**71%**	56%	63%	0%	2%	2%
DE	65%	**70%**	52%	2%	4%	1%
EE	66%	**75%**	44%	1%	5%	1%
IE	72%	**77%**	43%	1%	2%	1%
EL	62%	**68%**	64%	0%	3%	0%
ES	68%	46%	**73%**	0%	4%	1%
FR	56%	**77%**	57%	0%	1%	2%
HR	67%	**73%**	45%	2%	4%	2%
IT	**70%**	45%	**70%**	0%	5%	2%
CY	53%	**71%**	56%	1%	8%	2%
LV	**65%**	64%	61%	1%	2%	2%
LT	**75%**	69%	49%	0%	2%	1%
LU	64%	**81%**	46%	1%	2%	0%
HU	**66%**	58%	46%	3%	10%	2%
MT	42%	**81%**	66%	1%	2%	1%
NL	63%	**69%**	63%	2%	1%	0%
AT	60%	**74%**	57%	0%	2%	0%
PL	**74%**	73%	39%	0%	3%	3%
PT	53%	**75%**	52%	1%	8%	2%
RO	**75%**	71%	45%	0%	2%	1%
SI	71%	**72%**	42%	1%	5%	1%
SK	62%	**66%**	36%	1%	1%	3%
FI	**81%**	70%	44%	0%	1%	1%
SE	**72%**	57%	57%	3%	2%	0%
UK	**75%**	71%	40%	2%	2%	3%

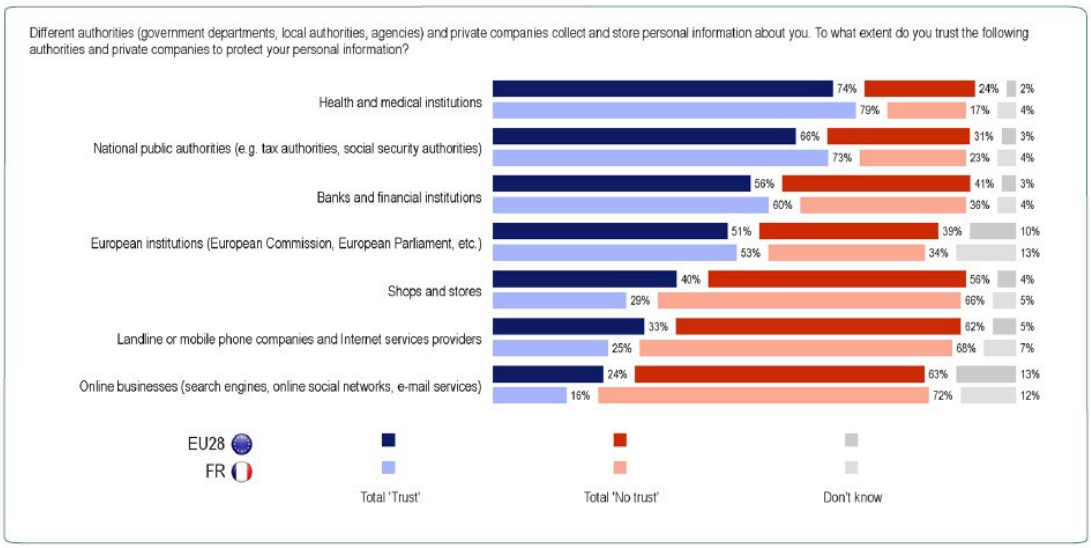
Highest percentage per country *Lowest percentage per country*

Highest percentage per item | Lowest percentage per item

Base: Respondents who provide information online (n=20,749 in EU28)

Annexe 17 : Confiance des populations de l'UE dans les différentes autorités responsables de la collecte et du stockage des données personnelles

Source : Eurobaromètre, 2015



Annexe 18 : Table : détail par État membre

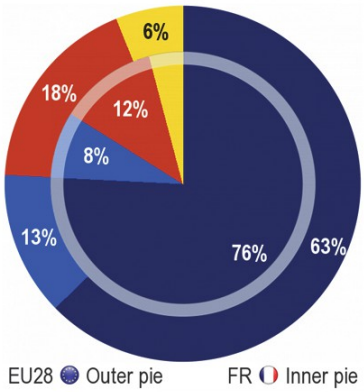
QB18. Different authorities (government departments, local authorities, agencies) and private companies collect and store personal information about you. To what extent do you trust the following authorities and private companies to protect your personal information?

	Health and medical institutions		National public authorities (e.g. tax authorities, social security authorities)		Banks and financial institutions		European institutions (European Commission, European Parliament, etc.)		Shops and stores		Landline or mobile phone companies and Internet services providers		Online businesses (search engines, online social networks, e-mail services)	
	Total 'Trust'	Diff. EB83.1-EB74.3	Total 'Trust'	Diff. EB83.1-EB74.3	Total 'Trust'	Diff. EB83.1-EB74.3	Total 'Trust'	Diff. EB83.1-EB74.3	Total 'Trust'	Diff. EB83.1-EB74.3	Total 'Trust'	Diff. EB83.1-EB74.3	Total 'Trust'	Diff. EB83.1-EB74.3
EU28	74%	-4	66%	-4	56%	-6	51%	-4	40%	+1	33%	+1	24%	+2
BE	85%	-6	79%	-1	66%	-11	67%	-6	43%	-8	37%	-1	22%	-1
BG	71%	-2	72%	-4	65%	=	59%	+5	38%	+10	39%	+4	26%	+6
CZ	75%	-4	73%	=	69%	-1	51%	-5	31%	-4	27%	-10	22%	-3
DK	89%	-4	86%	-6	89%	-3	67%	-4	52%	+5	46%	+2	35%	+3
DE	77%	-2	71%	=	57%	+1	47%	-1	39%	+5	32%	+12	19%	+3
EE	82%	-5	85%	+1	84%	-2	59%	-3	50%	-7	51%	-14	28%	-4
IE	73%	-7	72%	-2	59%	+6	57%	+1	54%	-2	48%	+7	39%	+10
EL	62%	+4	51%	-1	34%	+13	41%	-5	41%	+18	31%	+17	20%	+6
ES	74%	-11	49%	-20	33%	-26	42%	-19	46%	-1	18%	-9	19%	+1
FR	79%	-7	73%	-4	60%	-2	53%	-1	29%	-6	25%	-3	16%	=
HR	68%	NA*	54%	NA*	46%	NA*	54%	NA*	47%	NA*	35%	NA*	31%	NA*
IT	64%	-4	56%	-7	39%	-13	48%	-12	40%	+3	26%	-4	28%	+5
CY	69%	-9	59%	-5	44%	-30	42%	-5	45%	+2	53%	+3	25%	+13
LV	69%	-1	71%	+6	73%	=	49%	-2	40%	=	47%	-1	27%	-1
LT	73%	+2	68%	+5	73%	=	63%	+3	51%	+5	53%	+3	35%	+7
LU	85%	-5	82%	-6	77%	-9	70%	-3	38%	-1	45%	-4	27%	+10
HU	68%	-15	61%	-22	47%	-20	54%	-19	40%	+4	47%	-1	28%	+4
MT	87%	-2	75%	=	85%	-1	62%	+4	43%	+10	48%	-4	27%	+7
NL	81%	-2	82%	-2	74%	-5	63%	-1	31%	-2	37%	+7	18%	-2
AT	80%	+1	78%	-3	71%	-4	54%	-7	38%	+7	41%	+8	29%	+8
PL	61%	-2	60%	-1	58%	-3	55%	+1	35%	-1	37%	-5	29%	+4
PT	79%	=	64%	-12	50%	-14	54%	-11	46%	+6	29%	-3	24%	-2
RO	58%	-3	54%	-7	39%	-4	55%	-3	39%	+11	41%	+5	24%	+2
SI	75%	-7	62%	-9	64%	-15	60%	=	42%	-2	40%	+1	28%	+6
SK	72%	-12	70%	-12	73%	-7	60%	-13	41%	=	43%	-4	31%	-1
FI	90%	=	89%	+2	93%	+2	67%	+5	52%	-11	50%	-5	32%	-1
SE	88%	=	88%	+2	84%	-4	64%	-2	40%	-1	36%	+8	23%	-3
UK	81%	-2	69%	+6	70%	-5	44%	+6	46%	-2	45%	+2	32%	+2

Annexe 19 : Utilisation faite d'Internet par les populations de l'UE

Source : Eurobaromètre, 2015

D62R. Use of the Internet



EU28 Outer pie FR Inner pie

	EU28		FR	
	EB82.2	EB82.2 - EB79.4	EB82.2	EB82.2 - EB79.4
Every day	63%	+ 6	76%	+ 8
Often/ Sometimes	13%	- 2	8%	- 4
Never	18%	- 4	12%	- 4
No Internet access (SPONTANEOUS)	6%	=	4%	=

Evolution 2014 (EB82.2 10) - 2013 (EB79.4 05-06)

Annexe 20 : Fonctions pour lesquelles Internet est utilisé dans l'UE

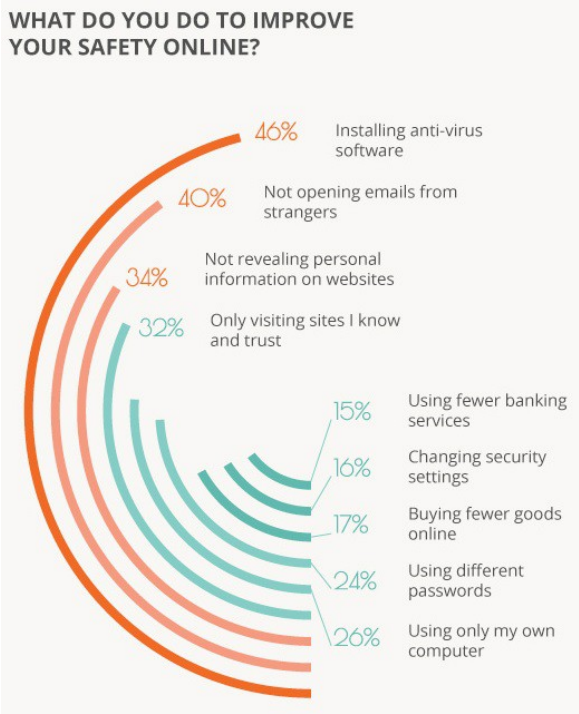
Source : Eurobaromètre, 2015

QB3. Which of the following activities do you do online? (MULTIPLE ANSWERS POSSIBLE)

Base: Internet users (n=21.015 in EU28)

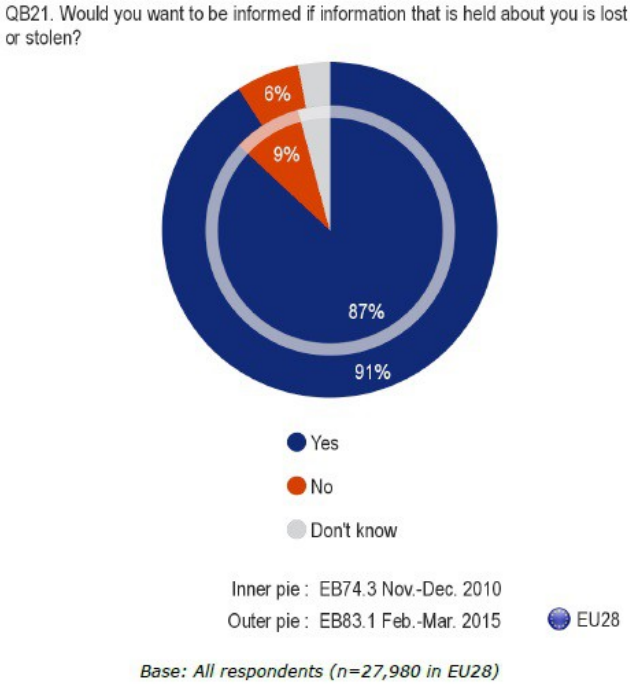
Annexe 21 : Réactions des populations de l'UE à la crainte d'être victimes de cybermenaces

Source : Eurobaromètre, 2013

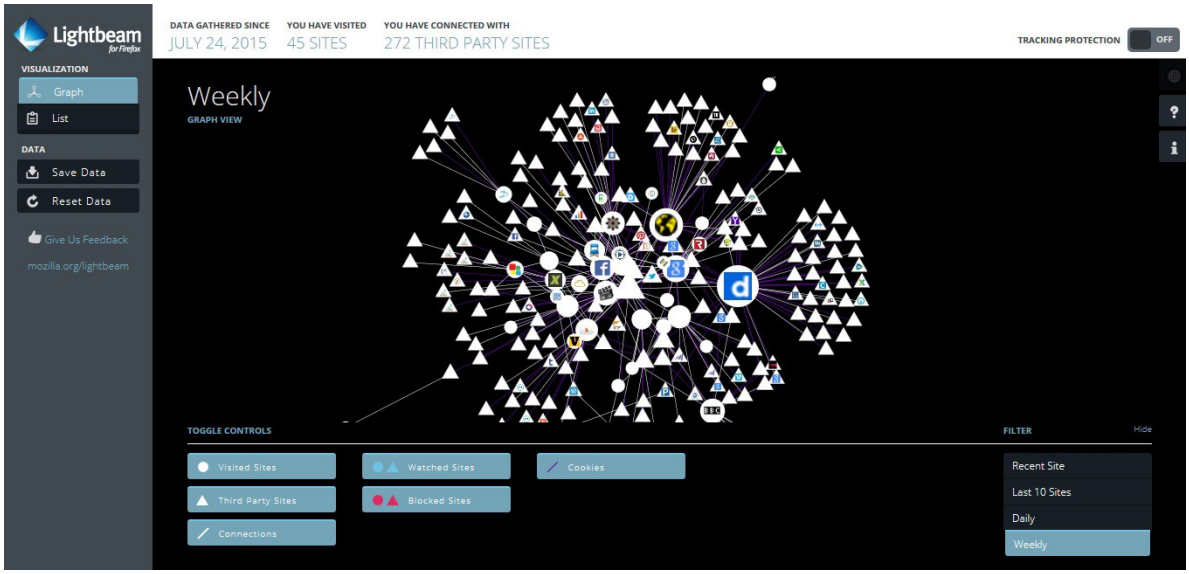


Annexe 22 : Positions sur la publicité des fuites de données personnelles

Source : Eurobaromètre, 2015



Annexe 23 : L'application *lightbeam* (capture d'écran)



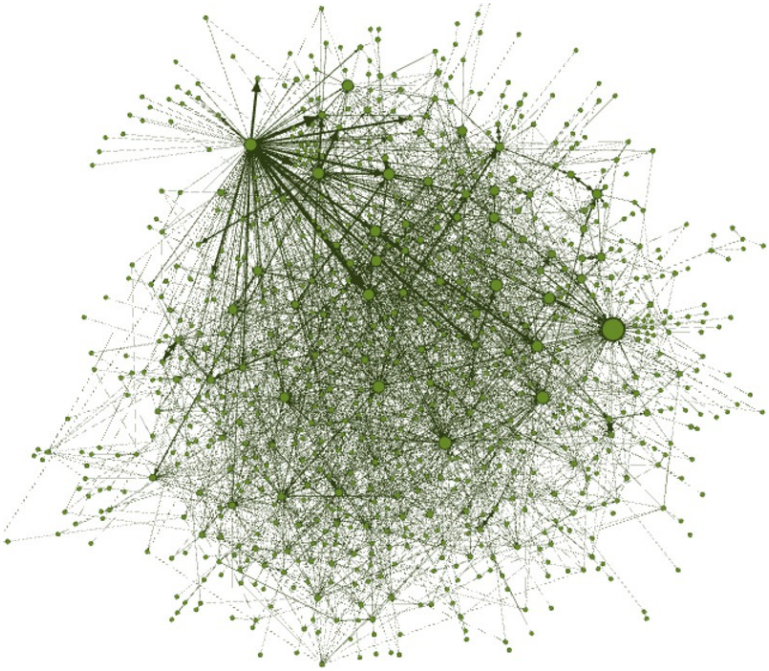
Annexe 24 : La page de présentation de *Cookieviz*, l'application proposée par la CNIL (capture d'écran)

Annexe 25 : Réseaux criminels : le modèle du gang

Source : Privacy, Security and Automation Lab (PSAL), l'université de Drexel, 2015

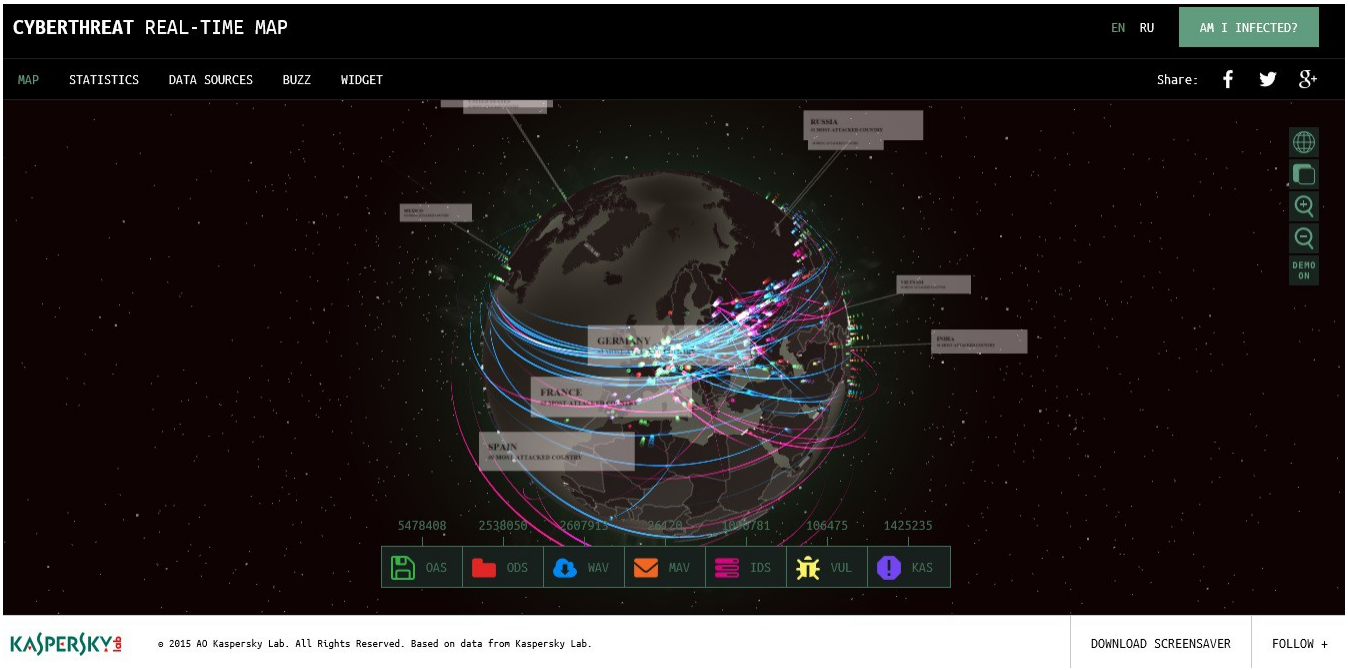
Annexe 26 : Réseaux criminels : le modèle du cartel

Source : Privacy, Security and Automation Lab (PSAL), l'université de Drexel, 2015



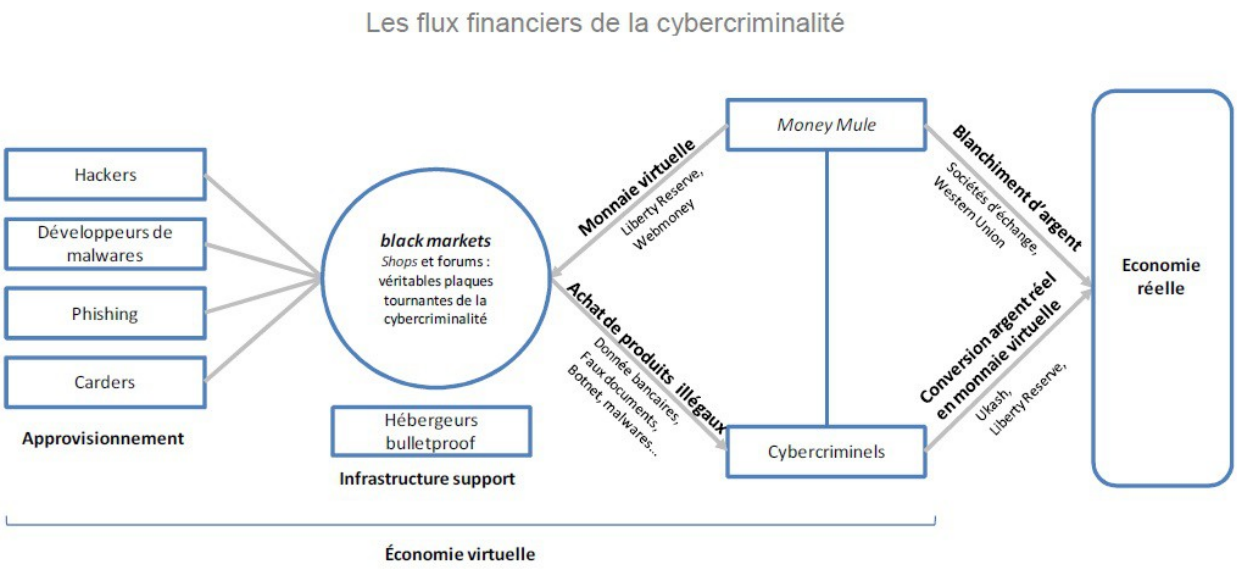
Annexe 27 : Carte en temps réel des cybermenaces

Source : Kaspersky, 2015



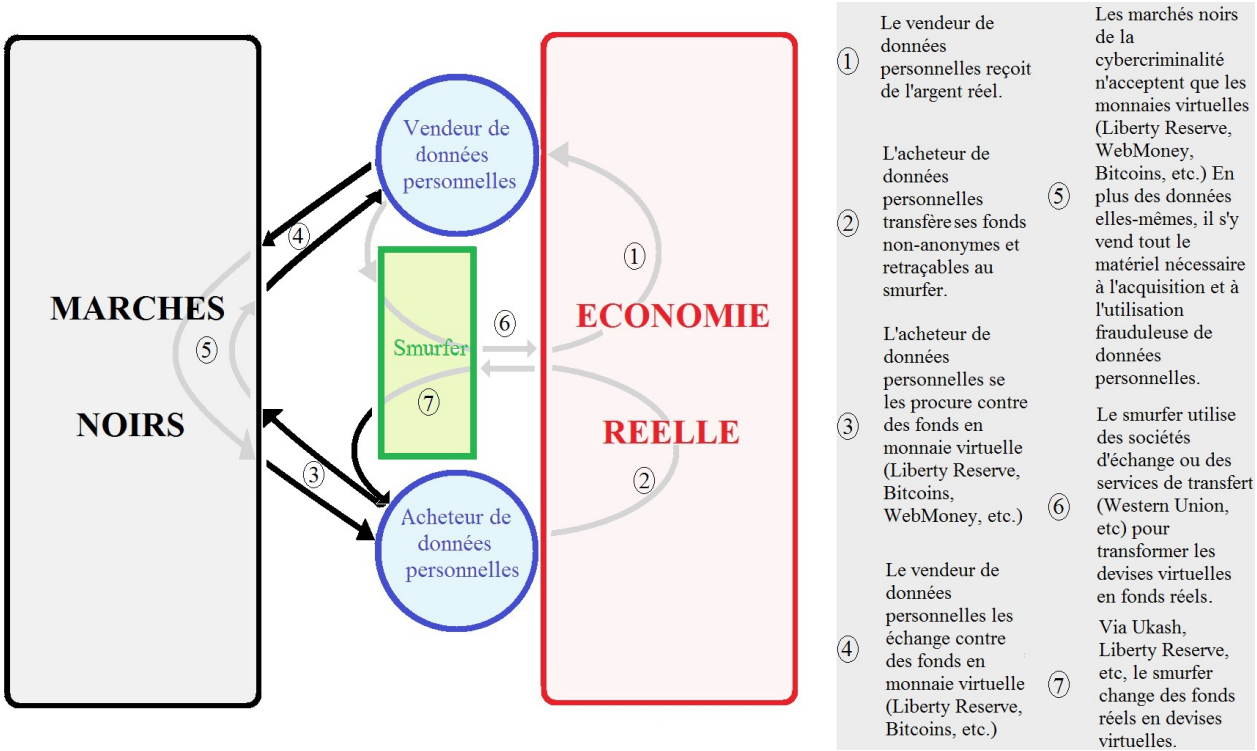
Annexe 28 : Le circuit financier de la cybercriminalité

Source : Compagnie Européenne d'Intelligence Stratégique (CEIS), 2011



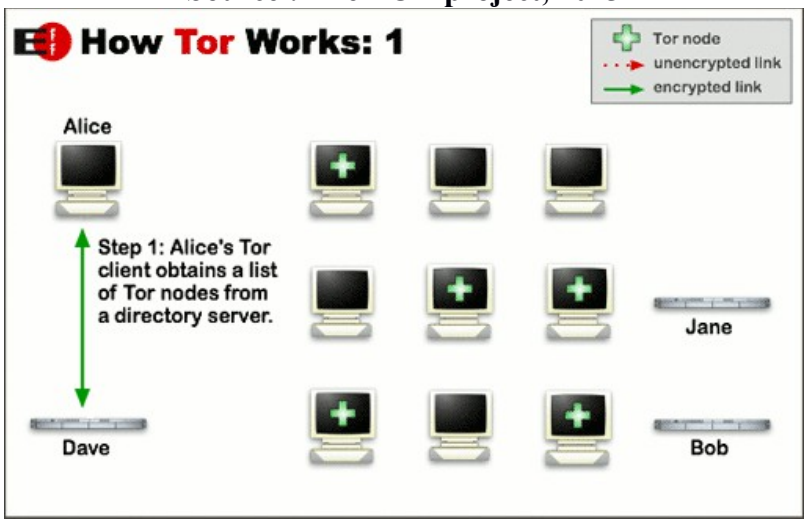
Annexe 29 : L'anonymisation des flux financiers de la cybercriminalité

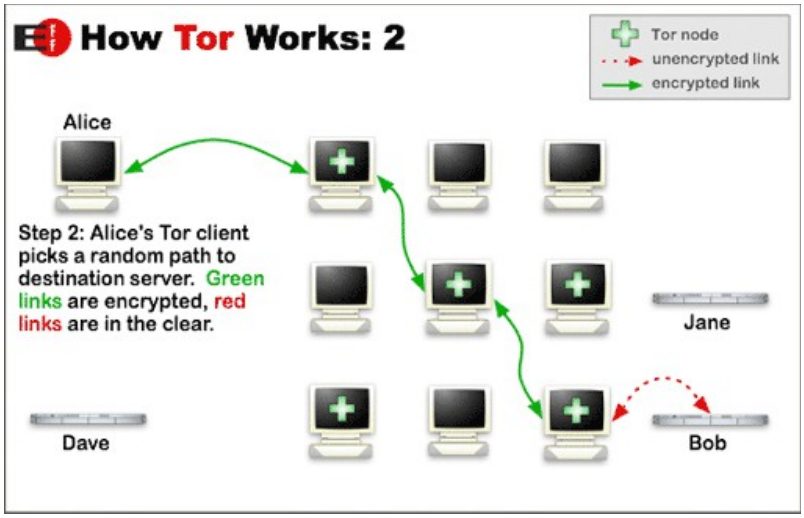
Source : schéma original

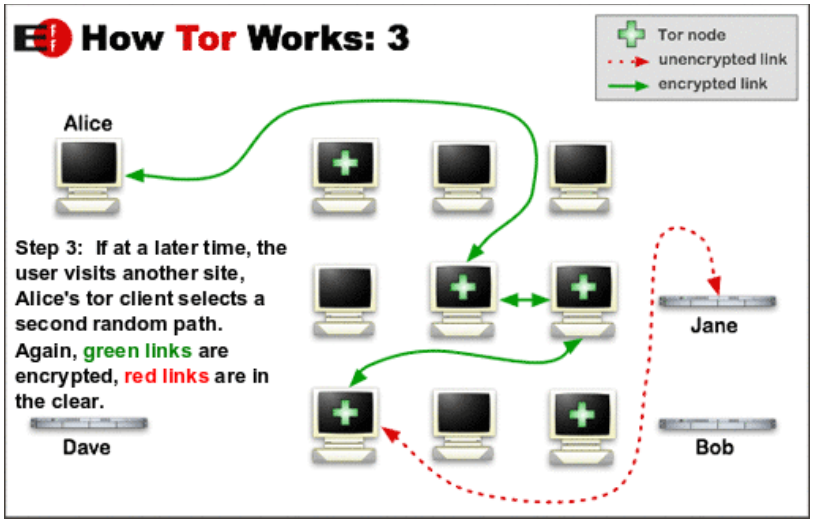


Annexe 30 : Schémas de fonctionnement de TOR

Source : The TOR project, 2015







Annexe 31 : Dix plus actifs pays émetteurs de *spams*

Source : Spamhaus, 2015

The Top 10 Worst

Countries | ISPs | Spammers

The World's Worst Spam Producing Countries

Most of the world suffers from the spam problem. However, some countries do little to deter spammers from operating within their borders. These countries become safe havens for the spam operations that plague everyone else, including their own nationals.

Countries with the highest number of spammers operating within their networks are usually those with poor or non-existent spam laws.

Source: Spamhaus Blocklist (SBL) database. Data is compiled automatically every 24 hours from the SBL database using the number of currently listed SBL records for each network (ISP/NSP) sorted by country.

The 10 Worst Spam Countries

As of 31 July 2015 the world's worst Spam Haven countries for production and export of spam are:

1	United States	Number of Current Live Spam Issues: 2743
2	China	Number of Current Live Spam Issues: 1341
3	Russian Federation	Number of Current Live Spam Issues: 962
4	Ukraine	Number of Current Live Spam Issues: 586
5	Japan	Number of Current Live Spam Issues: 585
6	United Kingdom	Number of Current Live Spam Issues: 382
7	India	Number of Current Live Spam Issues: 361
8	Germany	Number of Current Live Spam Issues: 342
9	Brazil	Number of Current Live Spam Issues: 336
10	Turkey	Number of Current Live Spam Issues: 321

Annexe 32 : Dix plus actifs hébergeurs *bulletproofs* émetteurs de *spams*

Source : Spamhaus, 2015

The Top 10 Worst

Countries | ISPs | Spammers

The World's Worst ISPs

The networks listed on this page knowingly provide service to criminal spam gangs and ignore spam reports from anti-spam systems and Internet users. These networks are defacto Spam Havens from where spammers operate freely and with the full knowledge of the network administrators and the executives. In the name of profits, these ten networks turn a blind eye to criminal spam gangs on their networks.

Spam continues to plague the Internet because a small number of large Internet Service Providers sell service knowingly to professional spammers for profit, or do nothing to prevent spammers operating from their networks.

Although all networks claim to be anti-spam, some network executives factor revenue made from hosting known spam gangs into corporate policy decisions to continue to sell services to spam operations. Others simply decide that closing the holes in their end-user broadband systems that allow spammers access would be too costly to their bottom lines.

The majority of the world's service providers succeed in keeping spammers off their networks and work to maintain a positive anti-spam reputation, but their work is undermined daily by the few networks such as these who, out of corporate greed or mismanagement, choose to be part of the problem.

SHARE

The World's Worst Spam Support ISPs

As of 31 July 2015 the ISPs with the worst Abuse Departments and consequently the worst reputations for knowingly hosting illegal spam operations are:

1	softlayer.com	Number of Current Known Spam Issues: 115
2	softbank.co.jp	Number of Current Known Spam Issues: 99
3	unicom-sc	Number of Current Known Spam Issues: 82
4	drpeng.com.cn	Number of Current Known Spam Issues: 65
5	unicom-bj	Number of Current Known Spam Issues: 64
6	gmo.jp	Number of Current Known Spam Issues: 49
7	chinanet-ah	Number of Current Known Spam Issues: 49
8	webexxpurts.com	Number of Current Known Spam Issues: 49
9	kddi.ne.jp	Number of Current Known Spam Issues: 44
10	kyivstar.net	Number of Current Known Spam Issues: 43

Annexe 33 : Dix plus actives opérations de *spamming*

Source : Spamhaus, 2015

The Top 10 Worst

Countries | ISPs | Spammers

The World's Worst Spammers

Up to 80% of spam targetted at Internet users in North America and Europe is generated by a hard-core group of around 100 known persistent spam gangs whose names, aliases and operations are documented in Spamhaus' Register Of Known Spam Operations (ROKSO) database.

This TOP 10 chart of ROKSO-listed spammers is based on those Spamhaus views as the highest threat, the worst of the career spammers causing the most damage on the Internet currently.

Source: Register Of Known Spam Operations (ROKSO) database + Spamhaus Blocklist (SBL) database. Detailed records on each spammer or spam gang listed can be viewed by clicking on the names.

The 10 Worst Spammers

As of 31 July 2015 the world's worst spammers and spam gangs are:

1 **Canadian Pharmacy** - Ukraine
A long time running pharmacy spam operation. They send tens of millions of spams per day using botnet techniques. Probably based in Eastern Europe, Ukraine/Russia. Host spammed web sites on botnets and on bulletproof Chinese web hosting.

2  **Dante Jimenez / Aiming Invest** - United States
Spamvaraz, lists, "bulletproof" hosting in the finest South Florida tradition. Working with worst cybercriminal botnet spammers. Now mostly involved in massive botnet spamming with hosting on hacked servers and Eastern European hosters.

3  **Yair Shalev / Kobeni Solutions** - United States
High volume snowshoe spammer from Florida, (former?) partner-in-spam of ROKSO spammer Darrin Wohl. Son-in-law of ROKSO listed spammer Dan Abramovich. Sued by FTC in 2014 due to fraud.

4 **Yambo Financials** - Ukraine
Huge spamhaus tied into distribution and billing for child, animal, and incest-porn, pirated software, and pharmaceuticals. Run their own merchant services (credit-card "collection" sites) set up as a fake "bank."

5 **Mike Boehm and Associates** - United States
Snowshoe spam organization that uses large numbers of inexpensive, automated VPS hosting IPs and domains in whatever TLD is currently cheapest to send high volumes of spam to extremely dirty, scraped lists. Operates under many business and individual names.

6 **Michael Persaud** - United States
Long time snowshoe type spammer.

7  **Michael Lindsay** - United States
Lindsay's iMedia Networks is a full-fledged spam-hosting operation serving bulletproof hosting at high premiums to well known ROKSO-listed spammers. His customers spam via botnet zombies with spam payloads hosted offshore, tunneled back to his servers. He and the gang have been hijacking (stealing) IP address space from companies for years to spam from. Illegal in the USA.

8 **Jagger Babuin / BHSI** - Canada
Romanian spammer now living in Vancouver BC. Also known as the "Dr Oz" spammer.

9 **First Place SEO & financial fraud spam gang** - United States
Seem to be either Northern New Jersey or San Diego, California based scammers. They rent endless numbers of servers and buy endless domains to then pump out "SEO", search-engine-rankings and financial fraud scam spams.

10 **Josh Henderson or Nicholson - bulletproofvps.com** - Canada
Offshore Bulletproof Hosting is his thing.

Annexe 34 : Tableau des types d'opérations répertoriées sur les 10 pires hébergeurs *bulletproofs*

Source : Spamhaus, 2015

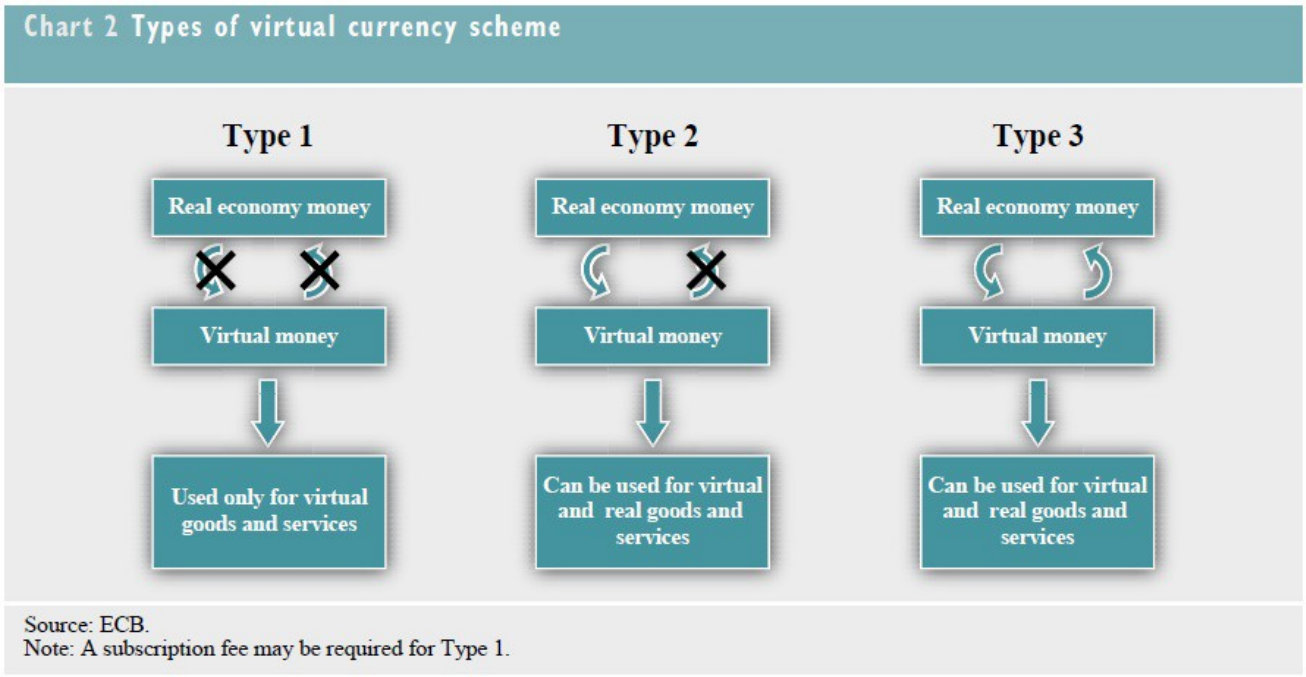
Position	10 pires hébergeurs *bulletproof*	Nombre l'éthiq	Nationalité									Envoi de spams	
1	*softlayer.com*	**115**	Etats-Unis	100	**87**			8	7	1	**1**	1	**1**
2	*softbank.co.jp*	**99**	Japon	2	**2**	19	**19**	7	7			64	**65**
3	*unicom-sc*	**82**	Chine	81	99								
4	*drpeng.com.cn*	**65**	Chine							12	**18**	46	**71**
5	*unicom-bj*	**64**	Chine			40	**63**	1	**2**			18	**28**
6	*gmo.jp*	**49**	Japon			1	**2**	16	**33**	10	**20**	16	**33**
7	*chinanet-ah*	**49**	Chine			25	**51**			19	**39**		
8	*webexxpurts.com*	**49**	Etats-Unis					2	**4**			29	**59**
9	*kddi.ne.jp*	**44**	Japon					20	**45**			16	**36**
10	*kyivstar.net*	**43**	Russie			32	**74**			5	**12**	1	**2**

Position	10 pires hébergeurs *bulletproof*	Nombre d'o l'éthique o	Nationalité	Sites de phishing						Utilisation comme proxy			
1	*softlayer.com*	**115**	Etats-Unis	4	**3**			1	**1**				
2	*softbank.co.jp*	**99**	Japon	2	**2**	1	**1**	3	**3**				
3	*unicom-sc*	**82**	Chine	1	**1**								
4	*drpeng.com.cn*	**65**	Chine	1	**2**	2	**3**	3	**5**	1	**2**		
5	*unicom-bj*	**64**	Chine	1	**2**	2	**3**	2	**3**				
6	*gmo.jp*	**49**	Japon	1	**2**	3	**6**	2	**4**				
7	*chinanet-ah*	**49**	Chine	1	**2**	1	**2**	3	**6**				
8	*webexxpurts.com*	**49**	Etats-Unis			1	**2**					17	**35**
9	*kddi.ne.jp*	**44**	Japon	3	**7**	1	**2**	4	**9**				
10	*kyivstar.net*	**43**	Russie			5	**12**						

Notes : la première colonne dans chaque catégorie contient le décompte du nombre d'opérations de ce type répertoriées et la seconde le pourcentage que représentent les opérations contraires à l'éthique et à la loi de cette catégorie parmi toutes celles répertoriées sur le serveur.

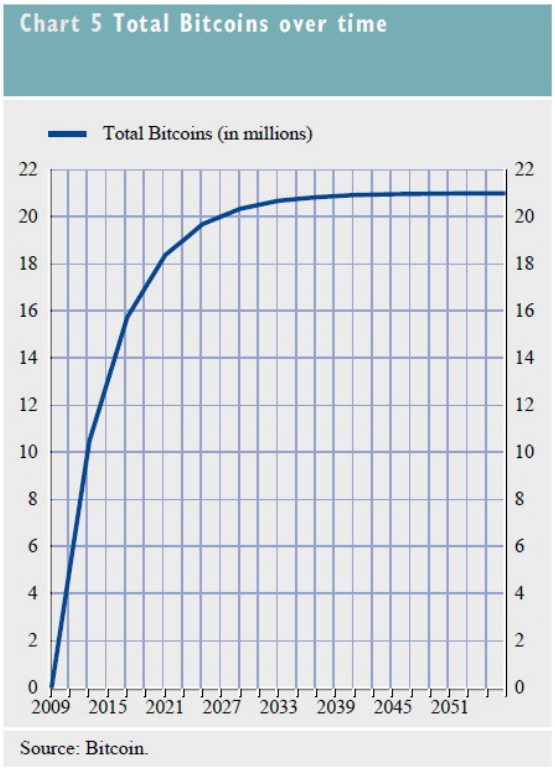
Annexe 35 : Les trois types de monnaies virtuelles selon la BCE

Source : Banque Centrale Européenne, 2012



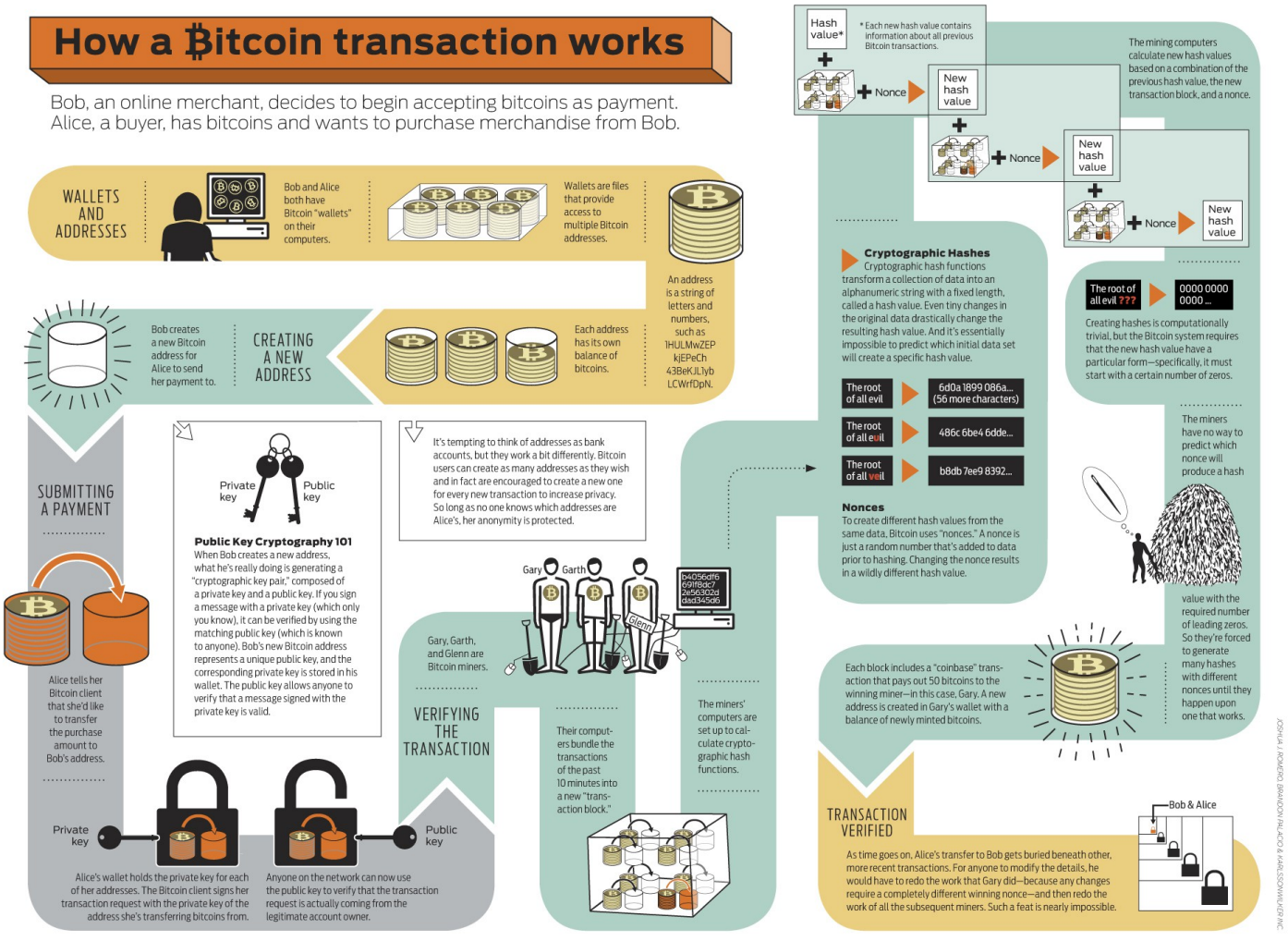
Annexe 36 : Projection du nombre total de *bitcoins* telle que présentée par la BCE

Source : Banque Centrale Européenne, 2012



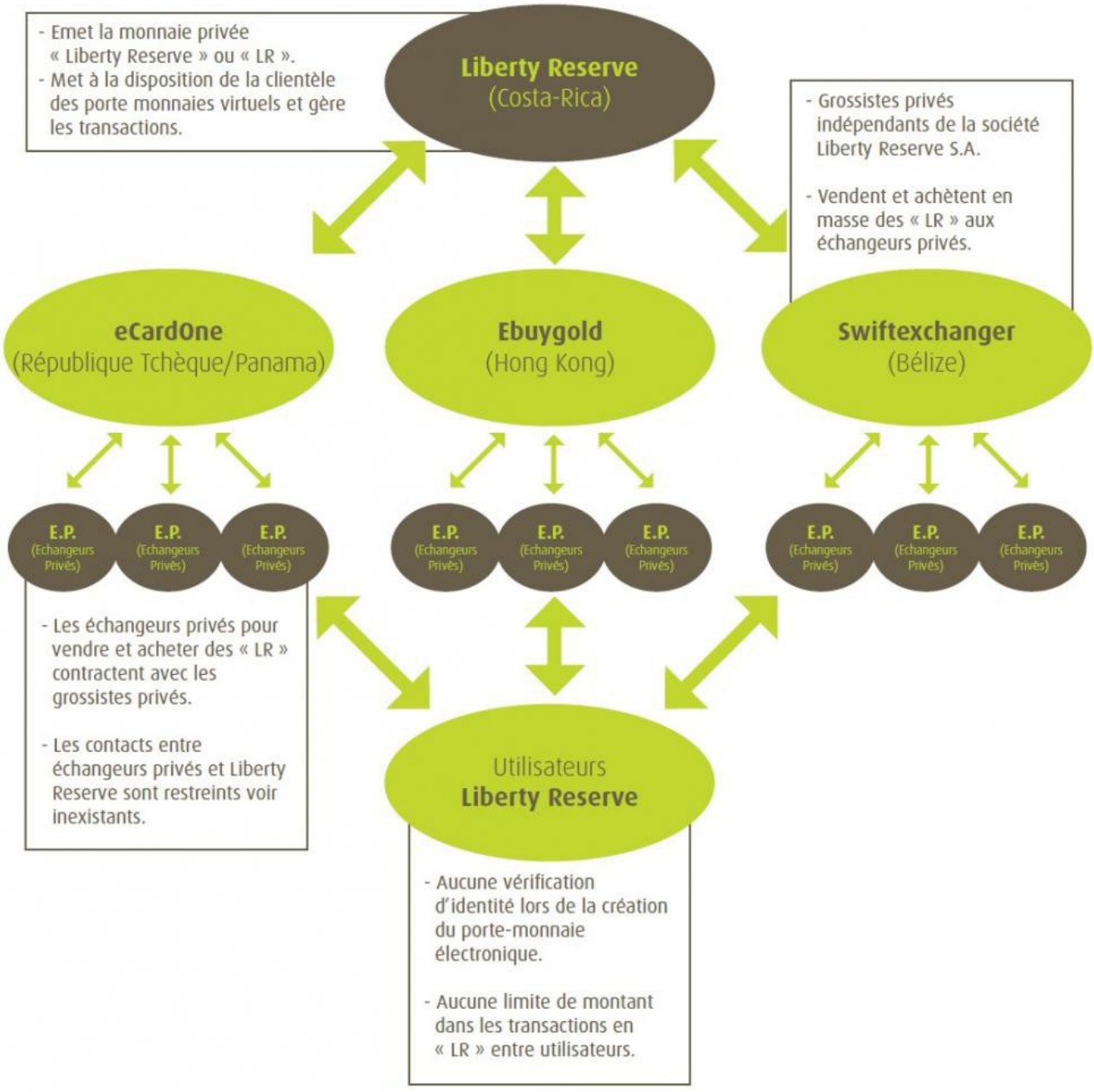
Annexe 37 : Fonctionnement de *Bitcoin*

Source : Joshua J. Romero, Brandon Palacio et arlssonwilker Inc., 2012



Annexe 38 : Fonctionnement de la monnaie virtuelle *Liberty Reserve*

Source : XMCO, 2011



Annexe 39 : Fonctionnement de Ukash

Source : Ukash, 2015

What's Ukash?

Ukash is eMoney. You treat it exactly like cash but spend it online. Perfect if you don't have a credit or debit card or don't want to use your card to pay online.

Getting Ukash is easy and convenient. Ukash is available at over 420,000 outlets worldwide, in over 55 countries. You can get Ukash from shops, petrol stations, kiosks, ATMs and online. Use our store locator to find your nearest outlet.

You simply exchange your cash for a unique 19-digit Ukash code. Don't worry if you're not sure how much to get. If your Ukash code is more than the value of the purchase you'll receive any change as a new code to use the next time you shop.

Ukash is safe and can be used immediately for secure payment. Your Ukash code can be used to pay at thousands of websites that accept Ukash. You can also load prepaid cards and eWallets.

Particuliers | Entreprises

my paysafecard login

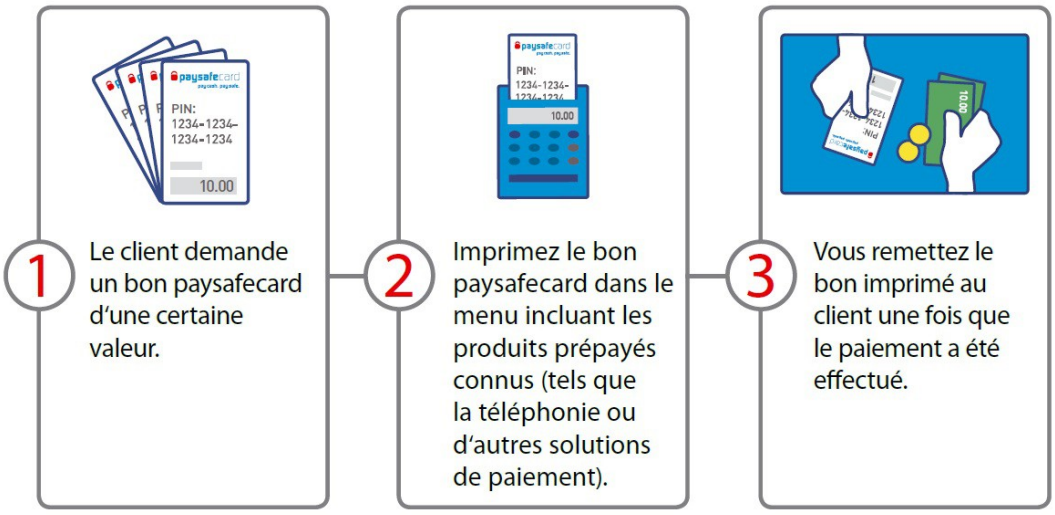
paysafecard
pay cash. pay safe.

Le produit | Acheter paysafecard | Utiliser paysafecard | Services | News

Ukash Services	Voici la marche à suivre avec paysafecard
Paiement avec le bon classique	Acheter simplement paysafecard dans le point de vente et introduire le code PIN à 16 chiffres lors du paiement
Combiner les codes PIN	Plusieurs codes PIN peuvent être combinés directement lors du paiement. Il suffit de les introduire dans les champs de saisie. Une inscription n'est pas requise dans ce cas.
Utiliser les montants restants	Les montants restants sur un bon restent valables et peuvent être utilisés ultérieurement. L'émission d'un nouveau bon avec le montant restant n'est pas nécessaire.
Compte Ukash	Avec my paysafecard, paysafecard met à votre disposition un compte personnel : • Les codes PIN peuvent être chargés dans le compte et être ainsi facilement gérés. • Avec my paysafecard, vous pouvez également payer directement en introduisant le nom d'utilisateur et le mot de passe. En savoir plus sur my paysafecard

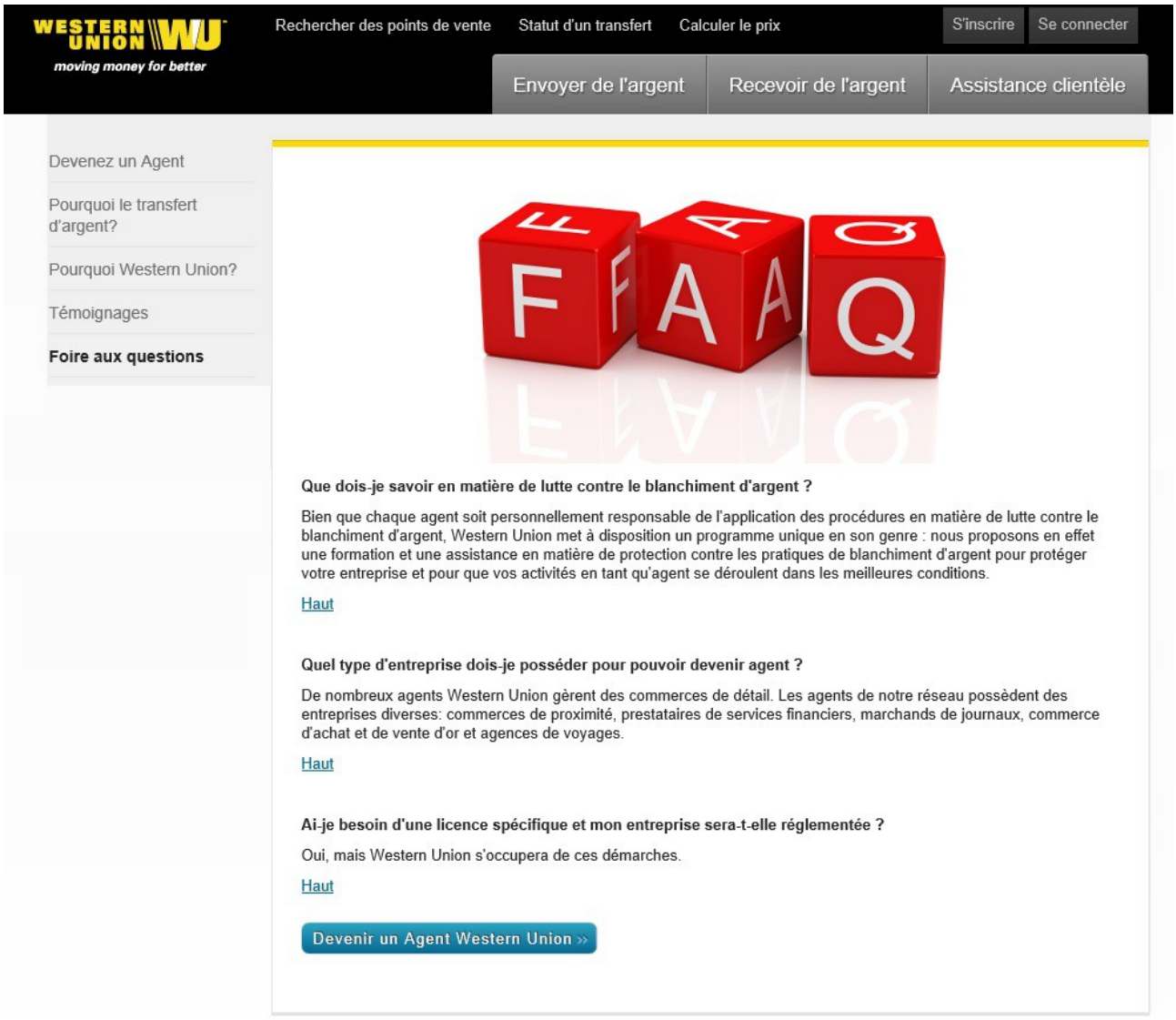
Annexe 40 : Conseils aux vendeurs Ukash pour la remise des bons

Source : Ukash, 2015



Annexe 41 : Politique de *Western Union* sur le blanchiment d'argent

Source : Western Union, 2015

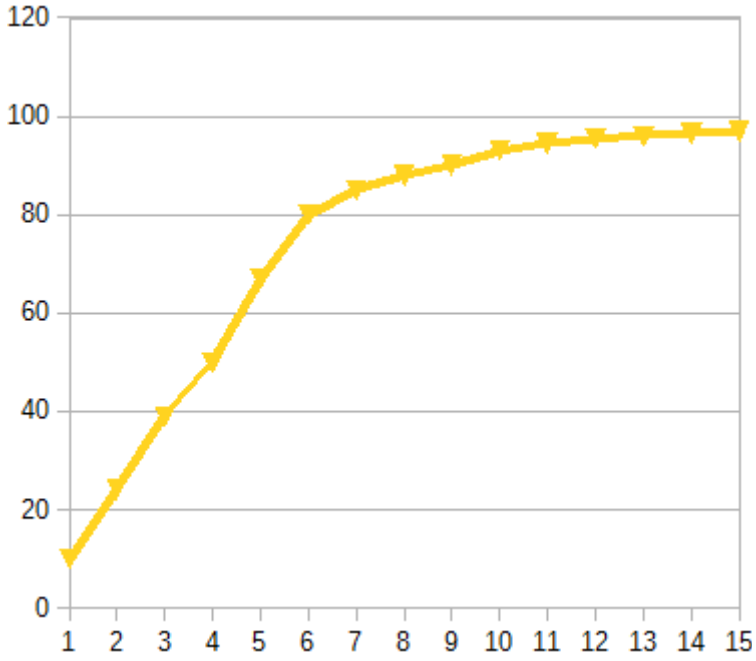


Annexe 42 : Le 23 février 2013, un usager de *PayPal* proteste sur le forum d'aide de la société, suite au gel de son compte
Source : forum d'aide *PayPal*, 2013

Annexe 43 : Les trois étapes de l'inscription sur *PayPal*
Source : PayPal, 2015

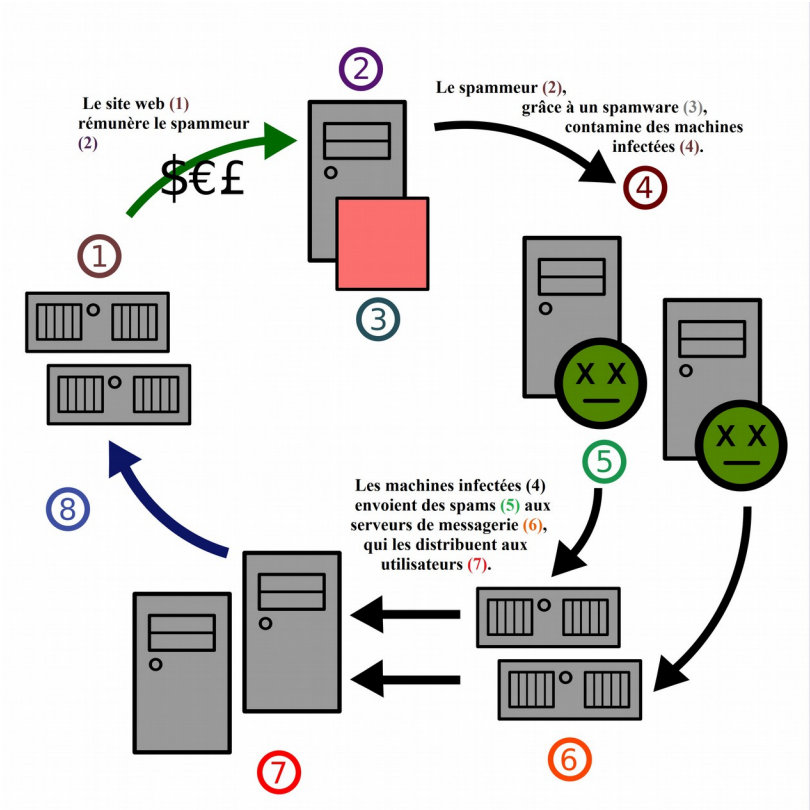
Annexe 44 : Projection du pourcentage des courriers électroniques qualifiables de *spams*

Source : Schéma original



Annexe 45 : Envoi d'un spam publicitaire

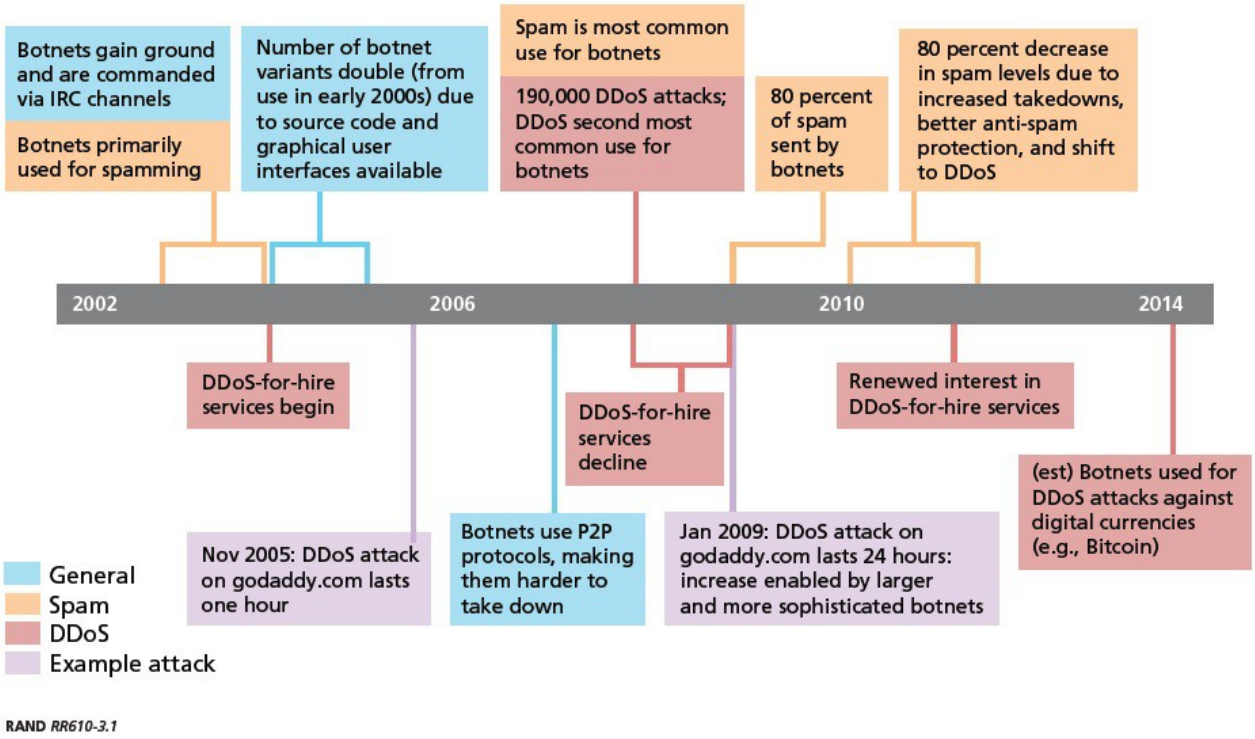
Source : schéma original



Annexe 46 : L'évolution du propos des *botnets* avec le temps

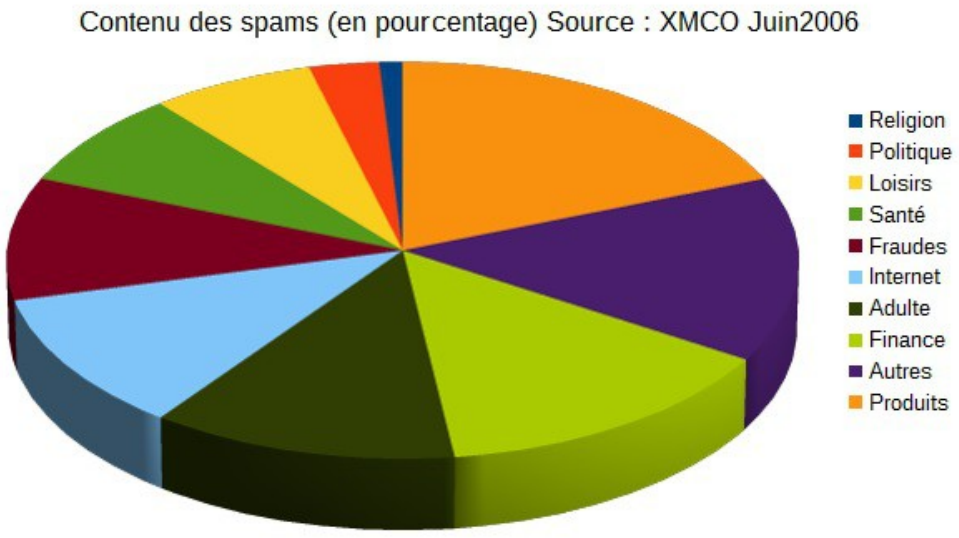
Source : Rand Corporation, 2014

Figure 3.1
Botnet Timeline

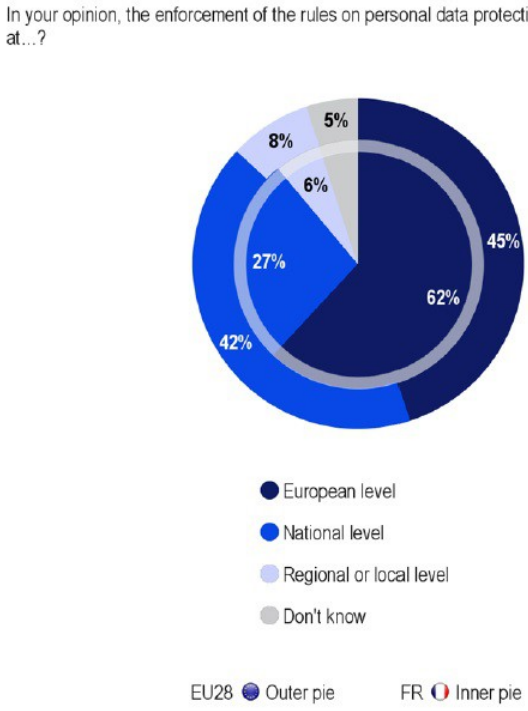


Annexe 47 : Contenus des *spams* (en pourcentage)

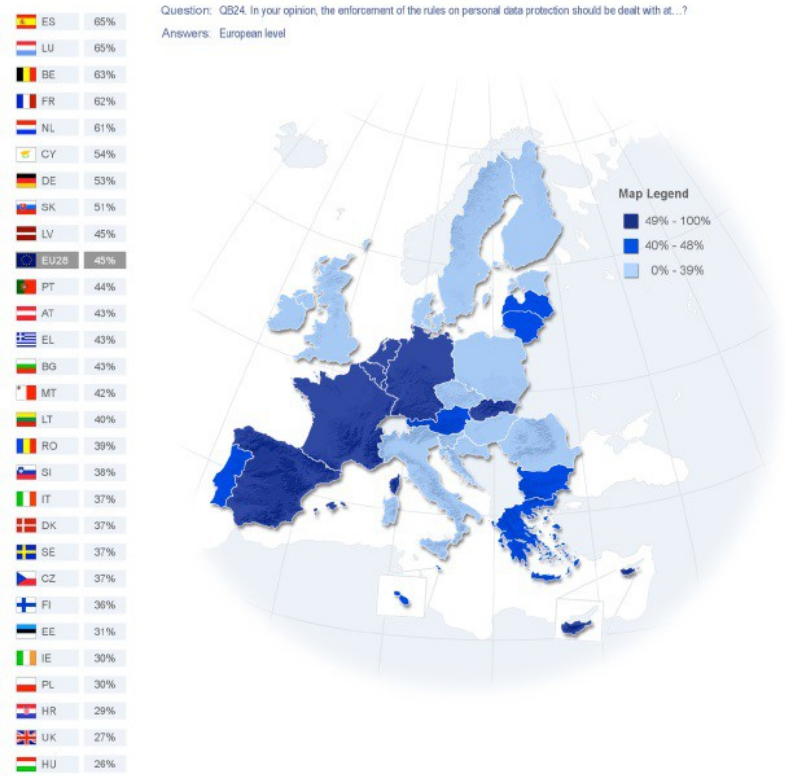
Source : XMCO, 2006



Annexe 48 : Réponses des populations de l'UE (cercle extérieur) et française (intérieur) à la question de savoir quelle autorité devrait gérer la protection des données personnelles
Source : Eurobaromètre, 2015



Annexe 49 : Carte de l'Union européenne de la volonté des populations de confier la protection des données personnelles à l'Union européenne
Source : Eurobaromètre, 2015



Annexe 50 : Matrice des risques des nouvelles méthodes de paiements

Source : GAFI, 2010

Critères		Liquide	NMP à haut risque	NMP à bas risque
Mesures de vigilance à l'égard de la clientèle	**Identification des clients**	Anonyme.	Anonyme.	Les utilisateurs sont identifiés.
	Vérification de leur identité	Anonyme.	Les utilisateurs ne sont pas identifiés de façon fiable et indépendante.	Les utilisateurs sont identifiés de façon fiable et indépendante.
	Surveillance des points de vente et sous-traitants	Aucune	Aucune	Surveillance en continu des relations commerciales
Tenue des registres		Aucune		Un enregistrement automatique est généré, conservé et rendu accessible aux autorités.
Limitation de la valeur	**Montant max. stockée sur un compte / nombre de comptes par personne**	Pas limité.	Pas limité.	Limité.
	Montant max. par transaction (incluant les dépôts et les retraits)	Pas limité.	Pas limité.	Limité.
	Fréquence max. des transactions	Pas limitée.	Pas limitée.	Limitée.
Méthode de financement			Source de financement anonyme (liquides, ordres de paiement, NMP anonymes) et sources multiples.	Financement depuis des comptes tenus dans une institution financière ou de crédit réglementées ou d'autres sources identifiées et soumis aux obligations et à la surveillance d'autorités financières nationales.

Critères		Liquide	NMP à haut risque	NMP à bas risque
Limites géographiques		Certaines devises sont utilisées plus largement que d'autres: les devises peuvent être changées par le biais d'intermédiaires.	Transfert de fonds ou retraits transfrontaliers.	Transfert de fonds et retraits seulement sur le territoire national.
Limitation de l'usage		Acceptées généralement.		Peu de commerçants et d'établissements bancaires les acceptant.
	Utilisation	p2b, b2b, p2p, pas d'utilisation en ligne.	p2b, b2b, p2p, utilisation en ligne.	p2b, b2b, utilisation en ligne possible, pas de p2p.
	Retraits		Retrait anonyme et illimité.	Limitation du montant et de la fréquence des retraits.
Segmentation des services	**Coopération entre fournisseurs de services**		Plusieurs fournisseurs indépendants accomplissent les différents étapes de la transaction sans vision à long-terme ni coordination.	Toute la transaction est réalisée par un seul fournisseur.
	Externalisation		Plusieurs étapes différents sont externalisées vers d'autres juridictions ne présentant pas les garanties adéquates, manque de vision à long-terme ou de lignes de responsabilités claires.	Tout le processus est réalisé en interne suivant des standards élevés.

Table des matières