Version 9 septembre 2014

Etude des bonnes pratiques

Les mécanismes de signalement en matière de cybercriminalité

Elaborée dans le cadre du projet GLACY

www.coe.int/cybercrime

Funded
by the European Union
and the Council of Europe

EUROPEAN UNION

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Implemented
by the Council of Europe

Sommaire

Note :

Le présent document a été élaboré par Jean-Christophe Le Toquin, SOCOGI, France, dans le cadre du projet GLACY relatif à l'Action globale sur la cybercriminalité.

Le résultat 6 du projet concerne le « partage de l'information : partage accru de l'information en ligne public/privé et inter-services, dans le respect des normes de protection des données » et la mise en œuvre des indicateurs suivants :
« Indicateurs objectivement vérifiables pour évaluer le degré de réalisation des objectifs & résultats / moyens des activités :

- mécanisme de signalement en ligne en relation avec les politiques relatives au partage de l'information des entités du secteur privé et les exigences existantes de la protection des données
- accords de coopération police/FSI adoptés dans pas moins de 10 pays
- pas moins de 10 pays ont les informations nécessaires pour mettre en place des mécanismes de signalement publics »

Cette activité part du principe que les dirigeants du secteur privé et les pouvoirs publics acceptent de coopérer dans le cadre qui sera établi. Leur engagement à cet égard devra être encouragé durant les activités de projet.

L'étude vient en particulier en appui à l'activité 6.4 : « Dispenser des conseils pour la création de mécanismes de signalement publics et de statistiques de la justice pénale sur la cybercriminalité ».

Elle soutient également deux activités distinctes mais néanmoins liées :

- 6.1 : Création d'une ressource en ligne (plate-forme) sur le partage d'informations privé/public et exigences de la protection des données (prévue en juin-décembre 2014)
- 6.2 : Soutien apporté à la création d'une base juridique pour le partage de l'information entre les services (notamment les services répressifs/CSIRT nationaux et privé/public dans le respect des normes relatives à la protection des données (prévu pendant toute la durée du projet, jusque mars 2016).

Les systèmes de signalement étudiés ont été sélectionnés pour leur réputation en termes d'efficacité, conjuguée à leur volonté de participer à l'étude. Les auteurs souhaitent ici remercier tous les experts qui leur ont consacré du temps et accepté de partager leurs informations confidentiellement.

1 Cadre et objectifs de l'étude

1.1 À propos du GLACY

D'une durée de 36 mois, le projet GLACY (Action globale sur la cybercriminalité) s'étend de novembre 2013 à octobre 2016. D'une portée mondiale, il est conçu comme une ressource pour aider de manière pragmatique les pays qui préparent la mise en œuvre de la Convention de Budapest sur la Cybercriminalité. Il est financé par l'Union européenne, en tant que mesure au service de la lutte contre le crime organisé du volet à long terme de l'Instrument de Stabilité, et soutenu par un cofinancement du Conseil de l'Europe.

Le projet GLACY vise à permettre aux autorités judiciaires pénales de s'engager dans la coopération internationale en matière de cybercriminalité et de preuve électronique sur le fondement de la Convention de Budapest sur la cybercriminalité. Plus généralement, il vise à poursuivre, au niveau national et international, l'harmonisation de la législation, de la formation et de la coopération dans la lutte contre la cybercriminalité.

Résultats attendus à la fin du projet GLACY :

- jusqu'à 70 pays sont engagés dans la lutte internationale contre la cybercriminalité en s'appuyant sur la Convention de Budapest comme cadre commun,
- la législation et les capacités des autorités judiciaires pénales ont été renforcées pour favoriser les enquêtes, les poursuites et le traitement des affaires en matière de cybercriminalité et de preuve électronique,
- la coopération policière et judiciaire internationale en matière de cybercriminalité et de preuves électroniques a été renforcée,
- les organisations des secteurs public et privé partagent leurs informations dans le respect des exigences de la protection des données,
- les progrès accomplis ont été évalués et les résultats obtenus seront intégrés dans les politiques et stratégies futures.

1.2 Objectifs de l'étude

Conformément aux objectifs du projet GLACY, la présente étude des bonnes pratiques porte principalement sur les mécanismes de signalement en matière de cybercriminalité. En partant de l'expérience de plusieurs systèmes établis à travers le monde, elle vise à apporter des conseils aux pays qui mettent en place leurs propres mécanismes de signalement en matière cybercriminalité, ou qui prévoient de le faire.

Bien que le projet soit financé et conçu pour soutenir un petit nombre de pays en Afrique et dans le Pacifique, la présente étude a son utilité pour tout pays qui prévoit de renforcer sa capacité contre la cybercriminalité.

1.3 Portée

La lutte contre la cybercriminalité relève en premier lieu de la responsabilité des autorités judiciaires pénales ; pour autant, le rôle du secteur privé, étant donné la nature extrêmement technique du phénomène et la nécessité d'une action rapide et efficace, ne doit pas être sous-estimé.

La motivation première des cybercriminels est le profit, principalement financier. Comme n'importe quelle entreprise légitime, les cybercriminels procèdent à des analyses coûts/bénéfices. Leurs activités ignorant les frontières juridiques entre droit pénal et droit

civil, elles relèvent des services répressifs et d'autres autorités publiques, notamment celles chargées de la protection des consommateurs et des données à caractère personnel.

Il est donc logique que la présente étude ne se limite pas aux initiatives établies et gérées par les services répressifs, mais s'intéresse aussi à celles d'autres autorités publiques et du secteur privé.

L'étude n'a aucune prétention d'exhaustivité en ce qui concerne les mécanismes de signalement en service en 2014. Les initiatives retenues sont représentatives des différents modèles de fonctionnement actuellement existants.

Quel que soit le mécanisme de rapport, deux éléments sont essentiels :

1. l'initiative : selon qu'elle est prise par le secteur public (en général la police ou les pouvoirs publics) ou par le secteur privé (association professionnelle ou ONG).

2. le financement : selon qu'il provient de fonds publics ou de contributions volontaires d'entreprises.

Ces deux éléments combinés permettent de dégager quatre types de mécanismes :

1. *Public* : mécanisme établi, géré et financé par le secteur public, avec un niveau de coopération plus ou moins important avec le secteur privé
2. *Public/privé* : mécanisme établi par le secteur privé, non viable sans le soutien financier du secteur public
3. *Privé/public*: mécanisme établi par le secteur privé, viable sans le soutien financier du secteur public, mais ayant besoin de la contribution du secteur public
4. *Privé* : mécanisme établi par le secteur privé, avec un niveau de coopération plus ou moins important avec le secteur public.

Les mécanismes étudiés peuvent être regroupés comme suit :

Initiative	**Mécanismes de signalement**
Public	Action Fraud, RU Consumer Sentinel Network (CSN), USA e-cops, Belgique Internet Signalement, France Cyber Security Mauritius, Maurice
Public/privé	National Cybersecurity Center (NCSC), Pays-Bas Internet Crime Complaint Centre (IC3), Etats-Unis INHOPE, Union européenne
Privé/public	Signal Spam, France
Privé	Anti-Phishing Working Group, Etats-Unis

1.4 Vue d'ensemble de l'étude

Lors de l'examen de la mise en œuvre d'un mécanisme de signalement en matière de cybercriminalité, le premier élément à considérer concerne les types de menaces qu'il devra couvrir. En général, un service répressif ou une autorité publique qui prévoit d'étendre ses activités du monde réel à l'environnement en ligne voit dans le mécanisme de signalement un moyen supplémentaire de recevoir des rapports électroniques. Il ou elle se met alors en quête du financement supplémentaire qui lui permettra de créer un mécanisme en ligne.

Cette approche organique a le mérite d'être simple, puisqu'il est inutile de classer les menaces par ordre de priorité au niveau national. Mais la création d'un nouveau mécanisme de signalement ne relève pas forcément de la décision d'un seul service, elle peut être décidée à un niveau plus élevé, dans un ministère ou même au niveau d'un gouvernement. Cette approche organique n'est alors pas forcément la mieux indiquée dans un pays qui ne dispose pas encore de mécanisme de signalement et qui a des moyens limités – le gouvernement national peut décider d'affecter des fonds publics à la lutte contre des menaces, s'il considère qu'il s'agit d'une priorité stratégique nationale. Dans ces conditions, le pays en question a tout intérêt à examiner les types de menaces auxquelles il veut s'attaquer en priorité. C'est l'objet de la section 2.

Une fois établie la liste des menaces que devra traiter le centre de signalement des cyber-délits, l'autre question à se poser concerne les résultats escomptés : quelle est la raison d'être du mécanisme, comment devrait-il être établi et quel devrait être son impact ? C'est ce que nous verrons à la section 3.

La section 4 revient plus en détail sur chacun des mécanismes examinés du point de vue de leurs avantages et de la manière dont ils contribuent au partage de l'information au niveau local et international.

La section 5, enfin, est une synthèse des enseignements tirés et rappelle une série de recommandations à l'intention des pays qui veulent mettre en place des mécanismes de signalement en matière de cybercriminalité.

2 Types de menaces devant être traitées par un mécanisme de signalement en matière de cybercriminalité

2.1 Définition

Dans la présente étude, le terme « cybercriminalité » est utilisé au sens large et englobe toute activité illégale poursuivie ou réglementée par le droit administratif, le droit civil et le droit pénal, qui vise des systèmes ou des technologies informatiques ou est commise par leur truchement.

2.2 Menaces et impacts

2.2.1 Menaces

La cybercriminalité est un concept très souple, toute activité illégale pouvant faire appel à des éléments électroniques, que ce soit pour sa préparation ou son exécution.

Chacun sait que les cybercriminels se jouent des frontières et qu'ils profitent de la territorialité des lois pour compliquer les enquêtes et les poursuites. S'il est vrai que la dimension internationale de la cybercriminalité représente un sérieux défi pour les gouvernements, une autre difficulté réside dans le fait que, dans chaque pays, les activités illicites ne font pas la différence entre organes répressifs, pouvoirs publics et sécurité nationale. Ainsi, un spam (message intempestif) peut-il faire partie d'une opération de hameçonnage (pour voler des données et de l'argent) envoyé via un ordinateur infecté par un ordinateur zombie (botnet), l'ordinateur étant lui-même utilisé pour des attaques décentralisées de dénis de service contre une infrastructure nationale sensible.

Concrètement, cela signifie que si les organisations, les autorités de régulation et les services de répression s'en tiennent scrupuleusement à leurs missions, la cybercriminalité brouille les lignes en permanence et contraint ces mêmes organisations, autorités et services à coopérer et à échanger leur expertise et leurs informations.

A cela s'ajoute que les technologies innovent en permanence et favorisent la mobilité : les salariés vont travailler avec leur propre matériel, sur lequel ils sauvegardent des données à caractère professionnel, tandis que les entreprises externalisent la gestion de leur parc informatique et transfèrent leurs données vers des serveurs dans le « cloud » hébergés outre-mer. « Internet everywhere », médias sociaux et applications mobiles font progressivement disparaître la frontière traditionnelle entre vie publique et vie privée. Les fraudeurs et les cybercriminels savent détourner toutes ces nouvelles opportunités à leur profit.

En règle générale, les menaces incluent les attaques contre :

- les particuliers – vol d'identité, vol de données à caractère personnel, réputation numérique, abus sexuel en ligne, incitation à la haine raciale
- les infrastructures – botnets et logiciels malveillants
- les biens – vol d'argent ou de données (données confidentielles ou contenus protégés par le droit d'auteur)
- la sécurité nationale – espionnage ou terrorisme.

Un pays qui veut établir son premier mécanisme de signalement en ligne en matière de cybercriminalité peut envisager de confier le projet à un service ou une autorité existante et de la laisser décider du meilleur moyen d'étendre ses activités au cyberespace.

Une autre approche, plus stratégique peut-être, consiste à étudier l'impact de la cybercriminalité sur le pays, et plus précisément sur la population, l'industrie et la sécurité nationale.

2.2.2 Impact sur la population

En général, les attaques contre les particuliers visent leurs données à caractère personnel et leur argent. Logiciels malveillants, spams, hameçonnage ou ingénierie sociale sont autant de moyens, parmi d'autres, utilisés pour voler des informations dans l'intention de commettre des fraudes, de voler l'identité ou de faire chanter des personnes (« sextorsion », par ex.).

L'impact de la cybercriminalité va donc de l'atteinte à la vie privée aux menaces contre l'intégrité physique et la vie des personnes (dans le cas de la commercialisation en ligne de scènes illicites d'abus sexuels).

Si l'impact financier de ces menaces est difficilement mesurable, un mécanisme de signalement est susceptible d'avoir un impact puisqu'on peut s'attendre à un nombre élevé de signalements.

2.2.3 Impact sur l'industrie

L'industrie est visée en relation avec les biens de valeur qu'elle contrôle (données confidentielles et protégées, argent). Botnets, logiciels malveillants, hacking, ingénierie sociale et collecte d'informations sont utilisés pour accéder à des informations protégées ou perturber son activité.

L'impact de la cybercriminalité va de la diffamation aux infractions à la propriété intellectuelle, des pertes financières directes ou indirectes au déni de service et au blocage du service et de la production.

En théorie, l'impact financier sur ces menaces est plus facilement mesurable, les autorités ayant affaire à un nombre nettement plus réduit de victimes, dont le personnel est capable d'évaluer les pertes et de communiquer avec les autorités.

La mise en place d'un mécanisme de signalement pour protéger les entreprises peut donc produire des résultats plus tangibles pour mesurer l'impact de la cybercriminalité, mais exige une compréhension approfondie, ainsi qu'une relation de confiance entre les autorités et les entreprises. Instaurer un niveau de confiance suffisant demande de la patience et une réelle volonté dans les deux camps, public et privé. Nul ne peut dire combien de temps il faut pour que la confiance s'instaure et le mécanisme de signalement peut considérer la collecte d'informations sur les menaces (ordinateurs infectés, système vulnérable, hameçonnage, etc.) comme un moyen d'ouvrir le dialogue avec les entreprises.

2.2.4 Impact sur les infrastructures nationales

Dernier point mais non des moindres, les infrastructures nationales (gouvernement, services de répression, pouvoirs publics, infrastructures sensibles) sont aussi la cible de criminels mus par des motivations politiques.

Un mécanisme de signalement n'est a priori pas adapté dans ce cas de figure, les victimes ne rendant compte qu'à leur hiérarchie via des procédures préétablies. Cela étant dit, la collecte de renseignements sur les menaces en ligne devrait être prise en compte, ne serait-ce que parce que des infrastructures comme les botnets sont polyvalentes et utilisées contre des particuliers, des entreprises et des infrastructures nationales.

Les cybercriminels étant actifs à l'échelle planétaire, toute mesure de lutte contre la cybercriminalité devrait s'inscrire dans un cadre plus vaste. Une collaboration public-privé renforcée et une implication plus grande des citoyens permettront de mieux comprendre les mécanismes et scénarii des cybercriminels, et de collecter des renseignements qui seront essentiels pour adapter les stratégies de lutte contre la cybercriminalité.

3 Bénéfices attendus des mécanismes de signalement en matière de cybercriminalité

À partir des entretiens réalisés pour la présente étude et des informations recueillies, cette section revient sur les raisons et les bénéfices qui justifient la mise en place des mécanismes de signalement.

Comme on va le voir dans les sections suivantes, la décision de créer des mécanismes de signalement peut être prise par le secteur public, le secteur privé, ou les deux combinés. En toute logique, leur mode de financement est variable – et joue un rôle décisif dans son fonctionnement, principalement sur la manière dont les données recueillies et les renseignements produits sont utilisés.

Le financement étant un élément déterminant de la décision de créer un nouveau mécanisme de signalement, l'étude analyse plusieurs initiatives du point de vue de leur modèle de financement, selon qu'il est public, public-privé, privé-public ou privé.

3.1 Objectifs des mécanismes de signalement

Les mécanismes de signalement étudiés indiquent généralement qu'ils ont été créés pour contribuer à une société de l'information qui soit sûre, ouverte et stable, et pour lutter contre ce qui est ressenti comme une augmentation permanente de la cybercriminalité.

Les objectifs des mécanismes de signalement sont d'ordre stratégique et opérationnel.

Objectifs stratégiques :

- disposer d'un outil de signalement centralisé et coordonner les actions des services de répression ou des pouvoirs publics dans un pays donné,
- démontrer que la réglementation applicable dans le monde réel s'applique aussi en ligne,
- sensibiliser les consommateurs et les entreprises, et proposer des outils éducatifs,
- coordonner les actions des secteurs public et privé.

Objectifs opérationnels :

- identifier les cyber-délits au niveau des pays et développer les capacités de répression,
- produire des statistiques sur les tendances et les menaces,
- enrichir les renseignements à partir de ces statistiques et mieux cibler les mesures de répression,
- partager l'information avec d'autres autorités nationales ou internationales de répression par le biais de publications, de rapports, de symposiums, etc.

L'objectif commun est de mettre en place un mécanisme de signalement inscrit dans une stratégie globale de lutte contre la cybercriminalité. Certains mécanismes de signalement couvrent un large éventail d'infractions (Action Fraud au Royaume-Uni, Internet Signalement en France, IC3 aux États-Unis, par ex.), tandis que d'autres ciblent des menaces spécifiques, comme APWG aux États-Unis (hameçonnage) ou Signal Spam en France (uniquement les spams au départ, aujourd'hui le hameçonnage et les botnets).

La plupart du temps, les citoyens et les victimes de cyber-délits ont accès à des mécanismes qui leur permettent de signaler facilement aux autorités pertinentes le préjudice qu'ils ont subi. Les données recueillies sont centralisées par le mécanisme de signalement avant d'être traitées par les organes répressifs et les autorités, qui peuvent suivre les tendances et prendre des mesures adaptées.

3.1.1 Mécanismes de signalement gérés par le secteur public

Les mécanismes publics étudiés ont été mis en place par les pouvoirs publics avec le soutien plus ou moins important du secteur privé.

3.1.1.1 Mécanismes mis en place par les services répressifs

En Belgique, **e-Cops**[1] a d'abord été créé pour lutter contre la pédopornographie sur Internet, après la révélation d'une affaire très grave de pédophilie en 1996. E-Cops, qui remplace le « point de contact central judiciaire » des débuts, recueille aussi des renseignements auprès de Child Focus, une fondation d'utilité publique pour les enfants disparus et sexuellement abusés. Son champ de compétence a évolué au fil des années. Aujourd'hui, e-Cops est le

[1] https://www.ecops.be/

point de contact unique pour les pratiques frauduleuses liées à Internet, y compris la pédopornographie, les fraudes sur Internet, la cybercriminalité ou le racisme, le but étant de bloquer les infrastructures illicites (sites Internet).

Le gouvernement français a créé **Internet Signalement**[2] pour permettre aux internautes de signaler des contenus violents et rassurer les citoyens sur le fait qu'Internet n'est pas une zone de non-droit. Mise en place par le ministère de l'Intérieur, la plateforme est le point de contact unique pour tous les signalements de contenus illicites et collabore avec de nombreux acteurs privés, notamment des hébergeurs, des plates-formes de réseau et des associations. Les signalements sont traités par des agents de police, jugés mieux placés pour prendre des mesures coercitives rapidement et mieux adaptées, surtout dans les cas les plus graves.

Face à la multiplication des mécanismes nationaux de signalement, la Commission européenne a créé en 2013 un **European Cybercrime Centre (EC3)**[3] au sein d'Europol. EC3 aide les Etats membres et les institutions européennes à mobiliser plus rapidement des capacités opérationnelles et analytiques dans le cadre des enquêtes et de la coopération avec les partenaires internationaux. Au niveau européen, EC3 est appelé à jouer un rôle majeur dans la lutte contre la cybercriminalité, en contribuant à des interventions plus rapides en cas de cyber-délits.

3.1.1.2 Mécanismes mis en place par les pouvoirs publics

Aux États-Unis, la Federal Trade Commission (FTC US) a démarré son activité de signalement en 1997, après avoir compris qu'elle pourrait tirer profit des plaintes des consommateurs à des fins de répression. FTC US est une agence indépendante du gouvernement des États-Unis, qui met à la disposition de la police un outil d'investigation électronique et une base de données des plaintes liées aux vols d'identité, à Internet, au télémarketing (y compris la liste anti-démarchage téléphonique), et d'autres plaintes de consommateurs. Des milliers d'agents des services de la répression civile et pénale aux États-Unis et à l'étranger ont accès aux informations reçues par la FTC, dont les spams, grâce à un site Internet sécurisé, **Consumer Sentinel Network (CSN)**[4]. La collecte, la gestion et l'analyse des données permet à FTC de mieux cibler ses mesures de répression, d'éduquer les consommateurs et les entreprises en vue de protéger la population, et d'identifier les tendances en matière de fraudes et d'infractions à la loi.

Le Royaume-Uni a créé **Action Fraud UK**[5] en 2010 dans le but de centraliser tous les renseignements sur les pratiques frauduleuses et la cybercriminalité. Le centre est soutenu par le gouvernement central (Cabinet Office, Home Office) et la Ville de Londres. Il propose un service de signalement unique pour les infractions et les informations relatives à la fraude et à la cybercriminalité à but lucratif.

Les données recueillies sont analysées par le National Fraud Intelligence Bureau qui, de par sa dimension fédérale, peut faire le lien entre plusieurs infractions à première vue sans rapport commises à travers le pays, offrant ainsi aux victimes un meilleur niveau de protection contre les groupes criminels organisés.

[2] https://www.internet-signalement.gouv.fr/
[3] https://www.europol.europa.eu/ec3
[4] http://www.ftc.gov/enforcement/consumer-sentinel-network
[5] http://www.actionfraud.police.uk/

Créé en 2008, le **Mauritian National Computer Security Incident Response Team (CERT-MU)**[6] est le principal centre national de coordination des renseignements sur les incidents en matière de sécurité dans le pays. Cette division du National Computer Board a pour mission d'informer et d'aider ses membres à prendre des mesures proactives pour réduire les risques d'incidents de sécurité qui touchent l'information, et à intervenir lorsque de tels incidents se produisent. Ses principaux objectifs sont : traitement et suivi des problèmes de sécurité dans les secteurs public et privé ; élaboration d'orientations à l'intention des fournisseurs d'informations sensibles pour qu'ils adoptent des bonnes pratiques en matière de sécurité de l'information ; sensibilisation et éducation des administrateurs systèmes et des utilisateurs aux derniers développements en matière de menaces sécuritaires et proposition de contre-mesures par la diffusion d'informations.

3.1.2 Mécanismes de signalement gérés par coopération public-privé

Les mécanismes de signalement ci-après sont des entités publiques ou privées ; aucun n'aurait pu voir le jour sans le leadership et le financement du secteur public.

Aux Pays-Bas, le **National Cybersecurity Center (NCSC)**[7] est une extension de la mission du CERT néerlandais. Le NCSC part du principe que l'échange d'information et la collaboration au niveau national et international sont importants pour favoriser la résilience numérique après l'affaire **DigiNotar** [8]. Le Centre surveille les activités des cybercriminels et coordonne les actions des services de répression. Pour le NCSC, collaborer avec le secteur privé permet de réagir plus efficacement en cas d'incidents de sécurité. Tout en étant une entité strictement publique, le Centre a fait de la coopération avec le secteur privé un élément central de son activité.

Le CSIRT (Computer Security Incident Response Team) a été créé au sein du NCSC et s'adresse aux organisations gouvernementales et aux infrastructures sensibles. Il intervient en cas d'incident informatique et propose des produits (outils, etc.) et services (notamment des alertes et des conseils) qui contribuent à la prévention, à la détection, à la réduction et au traitement des incidents, tout en réalisant des activités de sensibilisation.

D'après les informations du NCSC, il y a aujourd'hui plus de 250 CIRT dans plus de 70 pays et chaque année, de nouveaux centres d'alerte voient le jour. La coopération entre les CIRT est mondiale, informelle, et basée sur la confiance. Le NCSC néerlandais, qui héberge le CSIRT, se distingue toutefois des autres centres d'alerte en ce qu'il s'agit d'un partenariat public-privé spécialisé dans la sécurité nationale. A ce titre, il coordonne les opérations en cas d'incident ou de crise grave, susceptible de menacer la sécurité nationale, et notamment en cas de cyber-délits avec un impact national. Le NCSC collabore étroitement avec les autorités policières et judiciaires, des CSIRT étrangers, des instances publiques et des organisations privées au niveau national et international.

Le NCSC voit dans la coopération la clé de la réussite dans la lutte contre la cybercriminalité. Les CSIRT et les autorités de répression ont des missions et des pouvoirs bien distincts, mais œuvrent dans un même but – faire du monde numérique un endroit plus sûr. En unissant leurs forces, ils peuvent contribuer plus efficacement à la sécurité qu'ils ne pourraient le faire en agissaient chacun de leur côté.

[6] http://cert-mu.gov.mu/English/Pages/default.aspx

[7] https://www.ncsc.nl/

[8] Piratage de DigiNotar : une grave défaillance de sécurité à DigiNotar, l'autorité de certification néerlandaise, a été exploitée pour générer des certificats frauduleux.

Aux États-Unis, **Internet Crime Complaint Centre (IC3 US)**[9] a été établi en 2000 dans la cadre d'un partenariat entre le Federal Bureau of Investigation (FBI) et une organisation à but non lucratif, le National White Collar Crime Centre (NW3C). Centre d'appel au départ, IC3 a cessé cette activité en 2003 ; il n'accepte plus que les signalements en ligne.

IC3 propose un mécanisme qui permet aux victimes de délits sur Internet de signaler à la police de la juridiction concernée le délit dont elles ont été victimes. Les plaintes sont ensuite transférées aux services répressifs du niveau fédéral, de l'Etat, local ou international, et/ou aux organismes de réglementation, pour enquête.

Les signalements à IC3 servent un double objectif : d'une part, renforcer la capacité de répression en enregistrant les plaintes, et d'autre part, identifier les tendances de la cybercriminalité et établir des statistiques.

INHOPE[10] est une association internationale de 49 prestataires de dispositifs de signalement en ligne (hotlines) partenaires dans 43 pays. En partageant leurs connaissances, informations et bonnes pratiques, les membres du réseau INHOPE contribuent à lutter contre le problème mondial des contenus illicites sur Internet. Ses membres sont des organisations diverses (ONG, gouvernements, secteur privé) qui coopèrent avec la police, essentiellement pour lutter contre les contenus pédopornographiques. Le réseau a été constitué en 1999 par l'Union européenne, qui a apporté les fonds publics nécessaires pour que le projet puisse voir le jour.

Les hotlines d'INHOPE proposent des outils de signalement qui permettent aux citoyens de signaler des contenus illicites en ligne. Les hotlines ont accès aux signalements en fonction de leur législation nationale ; elles localisent le contenu et, s'il est hébergé dans leur pays, elles s'adressent soit à la police nationale pour enquête, soit au FSI pour qu'il bloque les contenus, soit à une autre hotline partenaire du réseau INHOPE.

9 http://www.ic3.gov/
10 http://inhope.org/

3.1.3 Mécanismes de signalement gérés par coopération privé-public

En France, **Signal Spam**[11] est une association à but non lucratif de lutte contre les spams qui propose aux internautes de signaler tout message qu'ils jugent non-sollicités ou frauduleux. Les membres de Signal Spam sont des autorités publiques (protection des données, police, etc.) et les acteurs de l'écosystème du courrier électronique (professionnels du marketing par courriel, fournisseurs de messagerie et vendeurs de systèmes de sécurité). Au départ, l'association avait pour mission d'aider l'autorité nationale chargée de la protection des données à renforcer sa capacité à réglementer les spams et à protéger les consommateurs contre les spams.

Les signalements sont recueillis et transmis aux membres de Signal Spam les mieux placés pour prendre les mesures qui s'imposent – l'autorité nationale chargée de la protection des données, la police, ou les expéditeurs des mails en cas de marketing légitime. Tous les signalements sont conservés et serviront de preuves en cas d'enquête officielle.

Signal Spam propose aussi des outils pédagogiques et partage toutes données utiles avec les acteurs concernés du marketing par courriel. L'association contribue également à diffuser les bonnes pratiques grâce à une charte déontologique à laquelle ses membres doivent obligatoirement respecter.

L'initiative public-privé, dirigée et financée par le secteur public, est devenue en 2010 une structure privée-publique. Signal spam est aujourd'hui financée uniquement par des fonds privés, mais elle est cogérée par des experts du public et du privé.

3.1.4 Mécanismes de signalement gérés par le secteur privé

Créé en 2003 aux États-Unis, **Anti-Phishing Working Group (APWG)**[12] était à l'origine un centre d'information pour les institutions victimes de hameçonnage (phishing). Les sites de hameçonnage sont signalés aux développeurs de navigateurs Web et aux entreprises de logiciels antivirus pour qu'ils fassent en sorte que leurs navigateurs et logiciels de sécurité bloquent les sites incriminés. Les signalements aident non seulement APWG à comprendre les tendances et à établir des statistiques, mais permettent aussi d'activer des notifications d'urgence : les notifications d'APWG aident à nettoyer les nœuds corrompus et à suspendre rapidement les noms de domaine frauduleux.

APWG est une coalition mondiale de lutte globale contre la cybercriminalité au sein de l'industrie, du gouvernement et des forces de l'ordre. Ses membres – plus de 2000 institutions réparties dans le monde – conseillent les gouvernements nationaux, des organes de gouvernance mondiale comme l'ICANN (Société pour l'attribution des noms de domaine et des numéros sur Internet), de grands groupes mondiaux et régionaux à vocation commerciale, ainsi que des organisations parties à des traités multilatéraux, dont la Commission européenne, la Convention du Conseil de l'Europe sur la cybercriminalité, le Bureau des Nations Unies contre la drogue et le crime (ODC), l'Organisation pour la sécurité et la coopération en Europe (OSCE) et l'Organisation des Etats américains.

3.2 Impact des mécanismes de signalement sur les réglementations et les pratiques économiques

[11] https://www.signal-spam.fr/
[12] http://www.apwg.org/

Quand on les interroge sur l'impact qu'ils ont sur le cadre réglementaire de leur pays, les mécanismes de signalement répondent qu'ils ont le sentiment de peser directement sur les pratiques économiques et les activités des services répressifs, plus que sur la réglementation elle-même.

S'agissant des services répressifs, les mécanismes de signalement estiment globalement contribuer à améliorer les procédures en faveur d'une coordination plus efficiente entre les services. Dès lors que des mesures sont appliquées plusieurs fois par différents services pour traiter un même délit commis sur Internet, le mécanisme de signalement favorise une coordination mondiale qui permet de réagir plus vite et mieux.

En ce qui concerne les pratiques des entreprises, plusieurs pays ont noté une amélioration de la collaboration entre les services répressifs, les autorités publiques, les associations professionnelles et les entreprises. C'est le cas de Signal Spam (France), qui a créé un écosystème composé des fournisseurs de messagerie, des organes de réglementation, des professionnels du marketing par courriel et des expéditeurs de courriels. La charte déontologique fixe en outre des règles qui ont abouti à l'exclusion des entreprises qui ne les respectent pas.

Si plusieurs mécanismes ayant des missions différentes en fonction du type d'infraction (abus sexuel commis sur des enfants, harcèlement moral, spam, hameçonnage et escroquerie, etc.) peuvent coexister dans un même pays, tous s'efforcent d'améliorer la coopération entre les services répressifs, les pouvoirs publics et le secteur privé. Ils collectent les plaintes des consommateurs ou des entreprises et les transmettent soit aux autorités concernées soit au mécanisme de signalement compétent. En 2010 aux États-Unis, IC3 a relayé 121 710 plaintes à la police et 2797 signalements de pédopornographie au National Center for Missing and Exploited Children.

Certains mécanismes de signalement alimentent une base de données centralisée. C'est le cas aux États-Unis, où le Consumer Sentinel Network sert de point de contact central auquel tous les services de police enregistrés ont accès. Les données sont collectées auprès des consommateurs et d'autres contributeurs externes, y compris d'autres mécanismes de signalement.

3.3 Impact des signalements sur les affaires pénales

Les organisations qui gèrent les mécanismes de signalement enregistrent un grand nombre de délits et de fraudes. Les données recueillies sont souvent une ressource très utile pour comprendre les tendances de la cybercriminalité et retrouver les criminels. Beaucoup de mécanismes de signalement coopèrent étroitement avec les autorités judiciaires et policières. Leur objectif répond en général à la nécessité de disposer d'un point de contact centralisé qui a valeur d'outil pour les autorités policières et judiciaires. Quand c'est possible, et en fonction de leur domaine de compétences, les plates-formes transfèrent les informations qu'elles reçoivent aux autorités compétentes. Pour comprendre la portée et l'importance de l'information avant de la transmettre aux services compétents, le mécanisme procède à une première analyse des contenus signalés.

Aux États-Unis, les données recueillies par les mécanismes de signalement alimentent une base de données centralisée par le **Consumer Sentinel Network** du FTC, à laquelle toutes les polices du pays ont accès.

Aux Pays-Bas, le **NCSC** a souligné que les CSIRT n'ont aucun des pouvoirs d'investigation dévolus aux autorités chargées de l'application de la loi. Ils ne peuvent prendre aucune

mesure coercitive, comme ordonner aux organisations qu'elles produisent ou bloquent des données, ou qu'elles ferment un site. Dans certains pays, la loi leur interdit même de partager leurs informations avec la police. Le NCSC pense néanmoins que les CSIRT peuvent être très utiles pour lutter contre la cybercriminalité en intervenant là où les autorités chargées de l'application de la loi rencontrent des difficultés. Les CSIRT sont de fait très précieux pour la coopération informelle basée sur la confiance. De plus, ils peuvent contribuer à la compréhension mutuelle des techniques et des outils utilisés par les criminels, en identifiant les principales menaces que représente la cybercriminalité et en agissant ensemble en faveur de la sensibilisation.

En France, **Internet Signalement** procède à une première vérification des informations avant d'orienter le signalement vers les enquêteurs des forces de police ou des instances judiciaires (des décrets gouvernementaux précisent les autorités concernées en fonction du type de contenu).

A sa création, **e-Cops** était une plate-forme judicaire de signalement judiciaire unique pour toute la Belgique, qui recueillait les signalements liés à l'exploitation sexuelle des enfants et à la criminalité économique. Cependant, son équipe n'a aucune capacité de recherche centrale (à l'exception des sites de hameçonnage hébergés en Belgique et des escroqueries avec transfert d'argent vers la Belgique). Après les avoir localisés, elle redirige les signalements valides soit vers le Service de lutte contre la traite de la police belge (s'il s'agit de cas d'abus sexuel commis sur des enfants) soit vers les partenaires locaux de la police. Les signalements liés à la criminalité économique sont transmis au Public Fédéral (SPF) Economie, qui a le droit d'enquêter et peut donc traiter les signalements comme des plaintes.

Action Fraud UK est un point de contact unique pour les fraudes et la cybercriminalité à but lucratif. Le service est dirigé par la Police de la Ville de Londres, qui travaille avec le National Fraud Intelligence Bureau (NFIB), l'organisme chargé d'évaluer les signalements et de s'assurer que les signalements parviennent au bon service. Comme ses homologues français et belge, le NFIB n'enquête pas sur les délits, mais fait suffisamment de recherches pour identifier le service qui devrait être chargé de l'affaire. En général, les délits sont traités par un service territorial de la police (souvent celui du lieu de résidence de l'auteur du délit). Le cas échéant, les signalements sont aussi transmis à des instances nationales, comme le Serious Fraud Office, le National Lead Force for Economic Crime (police de la Ville de Londres), la National Crime Agency, dont relève la National Cyber Crime Unit, et à des juridictions étrangères via Interpol. Le service intervient dans le respect de la loi sur la protection des données à caractère personnel et de la mission du service de police. La diffusion de l'information couvre un large éventail d'instances publiques et privées, dès lors qu'elle concerne la prévention de la criminalité et l'ordre public et qu'il est démontré qu'une action policière est nécessaire. Action Fraud contribue aux statistiques nationales sur la criminalité en communiquant au Home Office des informations détaillées sur les délits signalés.

Si ces plates-formes de signalement collaborent étroitement avec les autorités policières et judiciaires, elles n'ont en général aucune capacité de recherche approfondie. Leur travail d'investigation se limite à vérifier la validité des signalements, leur portée et leur localisation avant de les rediriger vers les autorités locales concernées, qui décident de la suite à leur donner. En France, **Internet Signalement** est considéré comme un acteur majeur du secteur français de l'Internet, en ce qu'il a une vue d'ensemble, en temps réel, des dernières tendances de l'Internet et de la cybercriminalité. **Internet Signalement** est régulièrement consulté par les groupes de travail législatif (y compris ceux établis par le gouvernement), mais ne prend pas part aux discussions sur les mesures pénales et n'est généralement pas

tenu informé des mesures que la police met en œuvre sur la base des informations qu'il lui a communiquées.

3.4 Sensibilisation

De l'avis des mécanismes de signalement étudiés, il est très important d'informer les citoyens et les entreprises de leur existence et de leur mission. Sensibiliser et éduquer les citoyens est essentiel pour garantir son succès. La sensibilisation et l'information montrent que le secteur public agit, seul ou en coopération avec le secteur privé, pour lutter contre la cybercriminalité et soutenir les consommateurs et les entreprises.

Il est souhaitable de mettre en place des mesures de communication et de sensibilisation dès la phase d'introduction du mécanisme de signalement, puis de les poursuivre en les adaptant.

Pendant la phase de lancement, on peut envisager d'utiliser les médias locaux (articles de presse, spots TV, affiches, etc.) pour lancer une campagne de sensibilisation. Certains pays utilisent d'autres outils intéressants, notamment :

- campagnes par SMS
- dépliants joints aux factures de téléphone
- campagnes dans les médias sociaux

Par la suite, de nouvelles activités de sensibilisation doivent être prévues pour asseoir l'efficacité du mécanisme de signalement à long terme. Les mécanismes existants font appel à divers moyens pour promouvoir leurs services :

- publications régulières de rapports
- communication via les médias sociaux
- partenariat avec les fournisseurs de services Internet (référencement sur les sites)
- articles réguliers dans la presse
- publication de messages d'intérêt général
- participation à des conférences et à des réunions nationales et internationales sur la cybercriminalité.

Au Royaume-Uni, les particuliers qui appellent les services de la police territoriale sont orientés vers **Action Fraud,** le cas échéant. Le mécanisme de signalement est présent sur Internet et communique avec la population via les médias sociaux.

Selon **Internet Signalement** (France), les campagnes de sensibilisation contribuent au succès du mécanisme de signalement. Une campagne de communication officielle a été menée en 2009. Depuis, Internet Signalement publie régulièrement des communiqués de presse et développe des partenariats avec de nombreux acteurs de l'Internet (entreprises et associations privées), s'assurant ainsi un meilleur référencement sur leurs sites.

Le mécanisme belge **e-Cops** est présent avec un lien sur la page d'accueil des fournisseurs de services Internet belges, sur plusieurs sites de commerce en ligne et sur d'autres sites.

3.5 Coûts d'établissement et dépenses de fonctionnement

Comme on peut s'y attendre, les coûts d'établissement et les dépenses de fonctionnement sont très variables d'un mécanisme de signalement à un autre, en fonction :

- de leur champ de compétence (mécanisme de signalement spécialisé/généraliste)

- de la méthode utilisée pour recueillir les signalements (procédure manuelle/automatisée)
- du nombre d'habitants dans le pays.

Les mécanismes étudiés variant par la taille, le champ de compétences et les missions, la présente étude ne peut donner que des tendances et des estimations. Les coûts englobent le matériel nécessaire à la construction de leur site Web, à la création et la maintenance d'une base de données, ainsi que la technique utilisée pour que les services répressifs puissent se connecter à l'outil de signalement pour trouver et traiter des informations.

La plupart des mécanismes sont financés uniquement ou principalement par des fonds publics. **Signal Spam** en France et **APWG** aux États-Unis sont des exceptions, puisqu'il s'agit d'initiatives privées entièrement financées par l'industrie. Ces entités à but non lucratif justifient les contributions et les cotisations de leurs membres par la qualité des informations qu'elles collectent et partagent avec les membres payants et le grand public.

3.5.1 Aperçu des plaintes traitées par les mécanismes de signalement en fonction de leur champ de compétences et du nombre d'habitants

La taille et le volume des signalements traités sont très variables, comme on peut le voir dans le tableau ci-dessous :

Pays	**Nombre d'habitants**	**Champ de compétences du mécanisme**	**Financements publics**	**Mécanisme public-privé**	**Mécanisme privé**
Royaume-Uni	environ 63 millions	Tous types de fraudes	Action Fraud : 229 018 fraudes traitées par la police et Action Fraud entre mars 2012 et mars 2013		
Belgique	environ 11 millions	Cybercriminalité uniquement	e-Cops : 24 220 plaintes reçues en 2011		
France	environ 66 millions	Internet Signalement : cybercriminalité Signal Spam: spams, phishing	Internet Signalement : 123 987 plaintes reçues en 2013		Signal Spam : 2 454 369 plaintes reçues en 2012
États-Unis	environ 314 millions	FTC : Tous types de fraudes IC3 US : cybercriminalité	FTC et Consumer Sentinel : 2 101 780 plaintes reçues en 2013	IC3 : 303 809 plaintes reçues en 2010	

3.5.2 Coûts

Calculer les coûts d'établissement et les dépenses de fonctionnement – souvent confidentiels – n'est pas une mince affaire. Les renseignements communiqués par les mécanismes de signalement permettent toutefois de donner une fourchette (à partir de 200 000 €).

- Création et maintenance du mécanisme de signalement : à partir de 200 000 €
  - mécanismes ayant un champ de compétences limité : Signal Spam (France) estime ses dépenses annuelles de fonctionnement à 200 000 € env. et APWG (États-Unis) à plus de 400 000 € ;
  - mécanismes de signalement recueillant tous types de fraudes : pour le Consumer Sentinel de la Federal Trade Commission (États-Unis), il a fallu sécuriser tout un bâtiment et acheter des équipements informatiques pour plusieurs millions d'euros.

- Personnel dédié : de 2 à plus de 30 personnes
  - une équipe réduite peut suffire pour les mécanismes spécialisés qui ont automatisé la procédure de signalement (comme Signal Spam en France, spécialisé dans le spam et le hameçonnage). Les projets plus lourds (FTC, IC3 US, Action Fraud UK, Internet Signalement France) ont besoin d'une équipe de 10 personnes minimum pour démarrer.

- Des spécialistes sont parfois nécessaires
  - si les plaintes sont analysées par des agents de la police générale (non spécialisés dans la cybercriminalité), ceux-ci doivent avoir des connaissances de base en informatique et dans le domaine de l'Internet. Les policiers devraient aussi être formés pour différencier les types de contenus et transférer les signalements aux autorités compétentes pour enquête ;
  - si les plaintes sont analysées par des unités spéciales, il faut une équipe de spécialistes de l'Internet et de la cybercriminalité.

- Infrastructures TIC
  - les coûts incluent : développement et maintenance du site Web, téléphones et lignes téléphoniques, connexion Internet, ordinateurs, imprimantes, photocopieurs, fax, système de gestion des signalements, sécurité (pare-feu, antivirus, connexion cryptée pour préserver l'anonymat des investigateurs qui visitent des sites suspects) ;
  - certains coûts ou équipements peuvent être pris en charge par des partenaires privés locaux (acteurs du secteur Internet ou donateurs privés). D'où l'importance de prendre contact avec eux dès le départ. Dans beaucoup de pays, il est possible de demander l'aide financière du gouvernement.

3.5.3 Exigences communes

À partir des contributions des mécanismes étudiés, on peut résumer les exigences communes comme suit :

- soutien politique/des dirigeants d'entreprises : le soutien du gouvernement ou de grands dirigeants est essentiel, quel que soit le mécanisme de signalement – on a ainsi l'assurance que le projet est perçu comme pertinent à tous les niveaux et on garantit le budget et le personnel nécessaire à la création et au fonctionnement du mécanisme ;

- personnel expérimenté :
  - un chef de projet TIC, pour mettre en place l'environnement informatique

- un responsable de la police qui sera l'interlocuteur de la direction en cas de problèmes pendant la phase de création et la phase d'exploitation du mécanisme de signalement
- des enquêteurs informatiques qui contribueront à définir la structure de travail du mécanisme
- des enquêteurs informatiques qui traiteront les plaintes avec l'aide d'assistants administratifs qui feront une première sélection ;

– soutien de la justice, car la police ne peut pas toujours décider des cas qui devraient être poursuivis.

3.5.4 Autres critères à prendre en considération

– La participation des internautes, qui peuvent aider à déterminer ce que les citoyens sont en droit d'attendre et pourquoi ils devraient signaler les fraudes ;

– la capacité à mesurer le retour sur investissement : les initiatives financées par des fonds privés jouissent d'une plus grande souplesse pour développer leur politique de tarification et leurs capacités, mais elles doivent pouvoir déterminer le retour sur investissement pour les membres payants.

3.6 Demande de soutien et promotion des bonnes pratiques

À l'exception notable d'INHOPE, aucun des mécanismes étudiés n'a mis en place de programme spécifique pour soutenir le développement de projets similaires dans d'autres pays.

En 2010, INHOPE a créé la Fondation INHOPE, qui soutient la création de nouvelles hotlines en dehors de l'Union européenne, principalement dans des pays qui tolèrent, produisent ou diffusent des contenus pédopornographiques. La Fondation se concentre sur les pays qui auraient besoin d'un mécanisme de signalement en ligne, mais où les moyens, la sensibilisation ou le soutien sont limités pour identifier, signaler, supprimer et/ou enquêter sur les contenus pédopornographiques sur Internet (2014-2015 : focus sur le développement de partenariats en Amérique latine, en Asie du Sud-Est et en Afrique).

La Fondation INHOPE conclut des partenariats avec des organisations nationales (principalement des ONG et des entreprises privées) dans les pays prioritaires qui disposent déjà d'une hotline ou qui veulent créer une hotline nationale. Les « participants » sont des organisations qui répondent aux critères de la Fondation en matière d'aide au développement. La Fondation apporte une aide « à la création » et propose au personnel des organisations qualifiées dans les pays ciblés une formation aux bonnes pratiques pour développer une hotline qui soit à même de traiter le problème des agressions sexuelles des enfants via Internet. Elle supervise également la phase de démarrage – elle donne notamment des conseils en matière de bonnes pratiques pour le recrutement du personnel, les besoins d'équipement, la sécurisation des lieux, la sauvegarde des données, ainsi que le développement de mesures internes et externes. S'agissant du financement, la Fondation ne peut apporter qu'un soutien limité et ne répond donc pas aux demandes de financement.

En 2013, INHOPE et Mobile Alliance Against Child Sexual Abuse Content (GSMA) ont publié un guide sur la création et la gestion d'une hotline[13], qui rappelle qu'« avant de mettre en place une hotline, il est capital que les citoyens comprennent bien le contexte national – en développant une compréhension approfondie de la législation locale, des attentes culturelles, de l'ampleur du problème, etc. ». Le guide contient une série de questions à se poser avant de se lancer. Les questions sont orientées sur les activités relatives aux contenus pédopornographiques, mais peuvent s'appliquer à tout type d'activité illicite susceptible d'être couverte par une hotline :

- Dans quelle mesure les critères juridiques des contenus pédopornographiques sont-ils clairement définis ?
- La législation existante est-elle adaptée ?
- Quelles sont les répercussions juridiques pour ceux qui regardent des images de contenus pédopornographiques sur Internet ?
- Une image cachée, créée automatiquement lorsqu'on la regarde, constitue-t-elle une infraction (autrement dit : cela revient-il à « créer » une image) ?
- De quelles dérogations une hotline/un collaborateur d'une hotline a-t-il besoin pour regarder un contenu potentiellement illicite dans le cadre de son travail ?
- La sauvegarde des données est-elle problématique (en relation avec les URL, les fichiers, ID des donneurs d'alerte / adresse IP) ?
- La préservation de l'anonymat de l'internaute est-elle problématique ?

[13] Hotlines: Responding to reports of illegal content online, octobre 2013, http://inhope.org/tns/news-and-events/news/13-10-14/Partnership_in_action_new_INHOPE_GSMA_resource_guide_the_ABC_on_how_to_set_up_and_manage_a_hotline_released.aspx

- Quelles sont les responsabilités juridiques de la hotline ? Que risque la hotline en cas de poursuites ?
- La hotline doit-elle être une entité/organisation humanitaire enregistrée ou équivalente ? Quelles sont les exigences juridiques en termes de propriété, de gouvernance, de transparence et de responsabilité ?
- Une hotline doit-elle être obligatoirement gérée par une autorité nationale (commission de surveillance cinématographique, autorité des médias et des communications) ?

INHOPE et GSMA recommandent d'obtenir le soutien et la participation d'acteurs extérieurs, dont :

- les pouvoirs publics : ils confèrent de la crédibilité au projet, peuvent apporter un soutien financier, autoriser la police à apporter les niveaux d'assistance nécessaires et revoir les législations si nécessaire.
- Autorités chargées de l'application de la loi : une collaboration étroite avec les services répressifs simplifie et renforce les processus de création et de fonctionnement de la hotline.
- Professionnels de l'Internet : amener les acteurs nationaux de l'Internet à comprendre et à partager les objectifs de la hotline facilite la suppression des contenus illicites ou le blocage des URL.
- Agences de protection de l'enfance (pour les contenus pédopornographiques) : elles pourront aider la hotline à obtenir l'adhésion d'acteurs clés (du gouvernement au grand public) et livrer des informations utiles sur la situation des initiatives visant les contenus pédopornographiques pendant le processus de développement de la hotline.
- D'autres hotlines ou INHOPE.

4 Vue d'ensemble des mécanismes de signalement étudiés

Le présent chapitre présente une vue d'ensemble des mécanismes étudiés :

- Belgique : eCops
- UE : European Cybercrime Centre (EC3), INHOPE
- France : Internet Signalement, Signal Spam
- Pays-Bas : Nationaal Cyber Security Centrum (NCSC)
- Royaume-Uni : Action Fraud
- États-Unis : Anti-Phishing Working Group (APWG), Internet Crime Complaint Center (IC3), Federal Trade Commission (FTC)
- Maurice : CERT-MU

4.1 Belgique : e-Cops

Site Web
https://www.ecops.be

Champ de compétences
• Signalement de pratiques frauduleuses sur Internet et de cyber-délits (même si le point de contact n'était pas vraiment prévu pour recueillir des plaintes) • Fermeture de sites pornographiques mettant en scène des enfants (focus sur les sites hébergés en Belgique) • Information des autres pays sur les « sites Web illicites » hébergés sur leur territoire • Sensibilisation des internautes aux dangers de l'Internet et aux actions possibles (documents d'information sur différentes thématiques)

Mode de signalement
Formulaire en ligne sur le site www.ecops.be

Partage de l'information	
Niveau national	Certaines statistiques de base sont partagées avec Child focus (Foundation for Missing and Sexually Exploited Children en Belgique)
Niveau international	Lorsqu'ils découvrent des sites pédopornographiques hébergés à l'étranger, les policiers envoient un rapport d'information policière de leurs découvertes (URL, nom de domaine, type de contenu illicite, etc.) au NCB d'Interpol du pays concerné. Pas de partage d'information avec des entités similaires dans d'autres pays.
Valeur informative *statistique* *opérationnelle* *stratégique*	• Analyse des tendances et des nouveaux phénomènes • Fermeture de sites Web frauduleux (sites de différents types - des sites hébergés en Belgique ont été fermés grâce aux signalements à eCops.
Accès public aux statistiques	Rapports annuels de la Direction contre la criminalité économique et financière depuis la création d'e-cops. 2007 (p. 100); 2008 (p. 94); 2009 (p. 95); 2010 (p.26), 2011 (p.32)

4.2 Union européenne : European Cybercrime Center (EC3)

Site Web	
https://www.europol.europa.eu/ec3	
Champ de compétences	
• Fraude en ligne • Abus sexuels commis sur des enfants • Autres formes de cybercriminalité	
Mode de signalement	
Pas de signalement direct. Liens vers les mécanismes nationaux de signalement (garantit un suivi par la police nationale).	
Partage de l'information	
Niveau national	EC3 n'est pas un mécanisme de signalement, mais une plate-forme de signalement pour les membres d'Europol qui peuvent y échanger leurs bonnes pratiques et coordonner leurs actions.
Niveau international	Avec les membres d'Europol, pour des actions coordonnées.
Valeur informative *statistique* *opérationnelle* *stratégique*	Analyse des données pour comprendre comment pensent et agissent les cybercriminels, les pédophiles et les fraudeurs. Leurs conclusions aident les services répressifs à cibler plus efficacement leurs opérations, mais pas seulement : EC3 est à l'origine de changements politiques et législatifs et surtout, est la référence pour conseiller les citoyens et les entreprises sur ce qu'il faut faire pour se protéger contre les menaces sur Internet.
Accès public aux statistiques	Non

4.3 Union européenne : INHOPE

Site Web	
www.inhope.org	
Champ de compétences	
Les contenus et activités illicites d'un point de vue pénal, avec un focus sur les contenus pédopornographiques. Les membres d'INHOPE peuvent aussi traiter d'autres types de contenus, en fonction de leurs législations nationales respectives.	
Mode de signalement	
Lien vers les hotlines nationales	
Partage de l'information	
Niveau national	Échange d'informations entre les membres d'INHOPE et avec les autorités nationales chargées d'appliquer la loi
Niveau international	Échanges de signalements entre les hotlines
Valeur informative *statistique* *opérationnelle* *stratégique*	• Analyse des données à des fins statistiques : analyse des dernières tendances et statistiques au niveau d'INHOPE et de ses membres • Les hotlines membres d'INHOPE partagent des informations avec les autorités nationales chargées de l'application de la loi concernées, pour d'autres actions
Accès public aux statistiques	Les statistiques de base sont publiées sur le site Web d'INHOPE. Les statistiques détaillées de chaque pays sont disponibles sur les sites Web des hotlines nationales.

4.4 France : Internet Signalement

Site Web	
www.internet-signalement.gouv.fr	
Champ de compétences	
Tous types de délits commis sur Internet	
Mode de signalement	
• Formulaire de signalement en ligne • Pour les professionnels, accès protégé spécial sur le site Web	
Partage de l'information	
Niveau national	Les données sont partagées avec les services répressifs
Niveau international	• Certaines informations sur des mineurs sont communiquées à Europol • Le réseau Interpol est utilisé pour informer sur des données illicites hébergées dans d'autres pays • Relation spéciale avec les pays francophones (Canada, Suisse, Belgique)
Valeur informative *statistique* *opérationnelle* *stratégique*	L'analyse des données contribue à : • identifier et analyser les nouvelles tendances de la criminalité • informer et alerter efficacement les citoyens et les professionnels • établir la typologie des contenus illicites sur Internet • mettre en œuvre des mesures préventives avec plusieurs partenaires

Accès public aux statistiques	Les tendances sont publiées sans commentaires particuliers

4.5 France : Signal Spam

Site Web	
https://www.signal-spam.fr	
Champ de compétences	
• Spam • Spambot • Hameçonnage • Scam • Marketing abusif par courriel • Marché gris du marketing par courriel	
Mode de signalement	
• Formulaire de signalement en ligne • Plug-ins pour les messageries clients	
Partage de l'information	
Niveau national	Beaucoup de données sont partagées avec les entreprises et entités locales.
Niveau international	Signal Spam partage ses informations avec des entités similaires ou des organismes officiellement reconnus d'autres pays.
Valeur informative *statistique* *opérationnelle* *stratégique*	Signal Spam recueille les signalements de spams des internautes, des statistiques agrégées des FSI, et remet des données stratégiques aux services publics.
Accès public aux statistiques	Rapports trimestriels : Octobre-Novembre 2013 Rapport annuel : 2012
Statistiques disponibles sur demande	Sur demande, Signal Spam communique des statistiques et des informations complètes sur un pays.

4.6 Pays-Bas : Nationaal Cyber Security Centrum (NCSC)

Site Web	
https://www.ncsc.nl	
Champ de compétences	
Reçoit, analyse et résout des incidents de sécurité sur le réseau (vulnérabilité logicielle, attaques virales et spécifiques).	
Mode de signalement	
Une équipe scanne Internet 24/7 à la recherche de menaces et de vulnérabilités numériques dans les systèmes logiciels et d'exploitation.	
Partage de l'information	
Niveau national	Système TARANIS : rapports consultatifs, e-mails hebdomadaires (fin de semaine), mails à une liste de diffusion interne, courriels et SMS d'alerte pour informer la population néerlandaise. Système BEITA : honeyspots (pots de miel) composés d'un réseau de renifleurs dans les organisations gouvernementales, donne aux instances gouvernementales un aperçu des menaces et de l'état du trafic réseau.
Niveau international	Coopération dans le cadre de la communauté mondiale des CSIRT
Valeur informative *statistique* *opérationnelle* *stratégique*	• Conseille la structure de crise nationale • Travaille étroitement avec les autorités policières et judiciaires, les autres CSIRT, les pouvoirs publics et des organisations privées au niveau national et international
Accès public aux statistiques	Fiches synoptiques et livres blancs disponibles sur le site du NCSC

4.7 Royaume-Uni : Action Fraud

Site Web
http://www.actionfraud.police.uk
Champ de compétences
• Fraudes financières et cyber-délits • Vol de véhicules • Comportement suspect avec ou à l'égard d'un enfant sur Internet • Documents ou messages d'incitation à la haine ou harcèlement • Vente de médicaments ou de matériel médical de contrefaçon sur Internet • Fraudes fiscales (entreprises ou particuliers) ou en relation avec le HMRC (Her Majesty's Revenue and Customs) • Fraude sociale • Fraude à l'immigration
Mode de signalement

Les deux principaux outils de signalement sont : • le téléphone • le site Web Sur le Web : • un outil global est à la disposition des entreprises publiques et des PME membres • un outil simplifié (Business Reporting Tool) garantissant un niveau plus élevé de connaissances sur les cyber-délits est également à la disposition des organisations publiques (gouvernementales) et privées • si l'auteur du délit est à côté ou si l'on pense qu'il est à proximité de la victime, celle-ci peut contacter la police locale (option « call for service »)	
Partage de l'information	
Niveau national	• Les statistiques et les informations complètes sont partagées avec la police et les services anti-fraude du pays • Les informations sont partagées avec un grand nombre d'instances publiques et privées dès lors qu'elles sont utiles pour la prévention de la criminalité (en vertu de la loi sur la protection des données) • lorsqu'il existe un besoin régulier de partager l'information et/ou de collaborer avec une organisation, le service s'efforce d'établir un accord de partage de l'information
Niveau international	• Le service partage activement ses renseignements avec des juridictions étrangères via les voies officielles (National Crime Agency à Interpol) • Il participe à plusieurs initiatives transfrontalières, notamment le groupe de travail international sur la fraude par marketing de masse
Valeur informative *statistique* *opérationnelle* *stratégique*	• Le NFIB utilise les données recueillies par Action Fraud pour proposer des analyses de renseignements qui serviront d'orientation stratégique et tactique • Il utilise aussi les rapports des établissements pénitentiaires pour recueillir des renseignements sur les criminels et formalise ses conclusions dans des documents qu'il partage avec l'industrie, afin de limiter les risques et supprimer les vulnérabilités systémiques dans les systèmes • Il trie les rapports sur la criminalité transmis par Action Fraud avant de les transférer à un service d'investigation. Le cas échéant, les rapports sont aussi transmis à des instances nationales (Serious Fraud Office, National Lead Force for Economic Crime (Police de la Ville de Londres), National Crime Agency (dont relève la National Cyber Crime Unit) et à des juridictions étrangères via Interpol.
Accès public aux statistiques	Le NFIB transmet les informations détaillées sur les délits enregistrés au Home Office, pour contrôle par l'Office of National Statistics

4.8 États-Unis : Anti Phishing Working Group (APWG)

Site Web	
www.apwg.org	
Champ de compétences	
• Hameçonnage • Toutes les formes de criminalité – infection des nœuds par des botnets, attaques de crimeware, hammeçonnage, etc. • Signalement de botnets uniquement – caractérisation approfondie du mode de corruption détecté • *URL Block List* d'APWG (UBL) • Bot-Infected Systems Alerting and Notification System (BISANS) • APWG Malicious Domain Suspension (AMDoS)	
Mode de signalement	
• Transfert les mails de hameçonnage à reportphishing@apwg.org • Formulaires en ligne à compléter (pour le grand public) • Téléchargement groupé des activités dans la base de données UBL qui utilise des services https	
Partage de l'information	
Niveau national	• UBL : toutes les données sont partagées systématiquement et automatiquement en mode 24/7 avec les membres – entreprises, ONG, CERT et les registres des TLD • BISANS : toutes les données sont partagées systématiquement et automatiquement 24/7 avec les membres – entreprises, ONG, CERT et FSI, ainsi que d'autres fournisseurs d'infrastructures Internet • AMDoS : les données de l'intervenant accrédité (qui fait la demande) sont communiquées au Registre
Niveau international	-
Valeur informative *statistique* *opérationnelle* *stratégique*	Tous génèrent des informations utiles à des fins statistiques, opérationnelles et stratégiques
Accès public aux statistiques	Rapports statistiques publics T3 2013

4.9 États-Unis : Consumer Sentinel Network

Site Web	
http://www.ftc.gov/enforcement/consumer-sentinel-network	
Champ de compétences	
• Plaintes de consommateurs relevant de la cybercriminalité • Pratiques frauduleuses, trompeuses et déloyales, dont : vol d'identité, fraude par télémarketing, fraude sur Internet et problèmes relatifs au crédit à la consommation.	
Mode de signalement	
Centre d'appel et formulaire de plaintes électroniques	
Partage de l'information	
Niveau national	Les agents de police enregistrés ont accès à la base de données
Niveau international	Non
Valeur informative *statistique* *opérationnelle* *stratégique*	Les plaintes des consommateurs reçues par le TFC, y compris les spams, sont à la disposition de milliers d'agents de la répression civile et pénale aux États-Unis et à l'étranger.
Accès public aux statistiques	Statistiques et rapports annuels

4.10 États-Unis : Internet Crime Complaint Center (IC3)

Site Web	
www.ic3.gov	
Champ de compétences	
Délits sur Internet en général, notamment : • en matière de droits de la propriété intellectuelle • piratage informatique (hacking) • espionnage économique (vol de secrets commerciaux) • extorsion en ligne • blanchiment d'argent international • vol d'identité	
Mode de signalement	
Signalement électronique sur IC3.gov	
Partage de l'information	
Niveau national	IC3 élabore des orientations à partir de ses données et les envoie aux services répressifs concernés au niveau local, de l'État, fédéral et international
Niveau international	IC3 envoie les orientations élaborées à partir des données des plaintes (uniquement) aux services répressifs des pays membres
Valeur informative *statistique* *opérationnelle* *stratégique*	• IC3 US remet des rapports statistiques à la hiérarchie du FBI • IC3 regroupe les plaintes de victimes pour en faire des affaires atteignent le seuil juridictionnel suffisant et les transfère aux services répressifs pertinents. • Les renseignements aident le FBI à anticiper les besoins et à prévoir les défis futurs de la cybercriminalité.
Accès public aux statistiques	Internet Crime Schemes Mesures de prévention Rapport annuel 2010

4.11 Maurice : Mauritian National Computer Security Incident Response Team

Site Web	
http://cert-mu.gov.mu/English/Pages/default.aspx	
Champ de compétences	
• Sécurité de l'information : incidents de sécurité et vulnérabilité dans les secteurs publics et privés (attaques DOS contre le portail du gouvernement et les FSI, opérations de hameçonnage contre les organismes financiers, etc.) • Atteintes à la vie privée • Harcèlement sur Internet • Programmes de sensibilisation et d'éducation	
Mode de signalement	
Formulaire électronique, e-mail, hotline, posts	
Partage de l'information	
Niveau national	Le CERT-MU traite les incidents causés à ses membres – FSI, universités, vendeurs de matériels informatiques, médias, services répressifs, particuliers, administrations et secteur privé.
Niveau international	Le CERT-MU est membre des organisations internationales suivantes : • CERT-CC • IMPACT • FIRST • APWG
Valeur informative *statistique* *opérationnelle* *stratégique*	• Alerte les internautes mauriciens en cas d'atteinte à la sécurité • Coordonne les avis des experts pour corriger le problème
Accès public aux statistiques	http://cert-mu.gov.mu/English/Pages/default.aspx

5 Conclusions/recommandations

La présente étude se propose de faciliter la mise en place de mécanismes de signalement en matière de cybercriminalité et le soutien du projet GLACY en la matière.

La cybercriminalité est un concept très souple, toute activité illégale pouvant faire appel à des éléments électroniques, que ce soit pour sa préparation ou son exécution. Il n'y a donc rien d'étonnant à ce que les mécanismes de signalement soient eux aussi « à géométrie variable » – ils recouvrent un large éventail de compétences, de rôles, d'initiatives publiques et/ou privées et de modèles de financement

Au-delà de leur diversité, les mécanismes de signalement ont en commun de contribuer aux mesures de lutte contre la cybercriminalité :

- en transférant les informations/plaintes exploitables, qui pourront servir de points de départ en cas d'enquêtes et de poursuites,
- en identifiant les menaces cybercriminelles qui pèsent sur les citoyens et les organisations, en appréhendant et en évaluant les tendances,
- en créant un outil de communication entre les citoyens (victimes/témoins de cyber-délits) et les autorités/initiatives responsables,
- en assurant la coordination en les autorités chargées de l'application de la loi et les pouvoirs publics,
- en encourageant une culture de la coopération et du partage de l'information public-privé.

Le projet GLACY se tient à disposition pour apporter d'autres conseils en matière de création des mécanismes de signalement publics et de collecte des statistiques judiciaires pénales sur la cybercriminalité. À ce stade, il convient de rappeler cinq recommandations essentielles :

1. Définir les principaux objectifs du mécanisme de signalement

Les cinq prestations susmentionnées sont autant d'orientations utiles pour définir les objectifs de tout mécanisme de signalement en matière de cybercriminalité.

La manière dont les signalements sont gérés par les différents services pour engager des poursuites est un élément décisif. Il convient en particulier de garder les deux points suivants à l'esprit :

- *Des enquêtes ou des poursuites seront-elles ouvertes sur la base des signalements ?* Recueillir des signalements uniquement pour comprendre des tendances est certes important, mais c'est insuffisant pour justifier pleinement la création d'un mécanisme de signalement. Donner les moyens d'une action répressive devrait faire partie intégrante de tout mécanisme de signalement.
- *Les signalements serviront-ils à améliorer la justice pénale sur une base permanente ?* Les autorités judiciaires et les initiatives du secteur privé ont des approches radicalement différentes. Alors que les initiatives privées veulent mesurer l'impact de leurs activités, en tirer des enseignements et améliorer leurs procédures, les services répressifs ont tendance à avoir une approche plus linéaire, où les signalements sont reçus et traités avec efficacité et diligence. Un mécanisme de signalement est aussi un outil qui permet de mesurer et d'améliorer l'efficience

de la justice pénale. L'un des intérêts à long terme des mécanismes de signalement est d'améliorer le cadre juridique afin d'aider les services gouvernementaux à lutter plus efficacement contre la cybercriminalité.

2. Concentration sur les principales menaces

Comme nous l'avons vu au chapitre 2, des pays peuvent être touchés par différents types de menaces, avec des niveaux d'impact différents. La création d'un centre de signalement implique par conséquent de se concentrer sur les principales menaces, les plus importantes, car il est quasi impossible pour un mécanisme de signalement, surtout au début, de traiter toutes les formes de menaces.

A cela s'ajoute qu'en se concentrant sur les principales menaces majeures, le mécanisme de signalement gagne en crédibilité.

3. Garder l'esprit ouvert

Un service de répression qui met en place un mécanisme permettant les signalements électroniques peut être chargé de traiter des menaces spécifiques et dans ce cas, il acceptera uniquement les signalements des délits qui le concernent.

D'un autre côté, un gouvernement qui veut créer un mécanisme de signalement ouvert à toutes les formes de menaces sur Internet pourra se faire une idée intéressante des préoccupations des citoyens et des entreprises, et prévoir une réponse mieux adaptée et mieux ciblée pour contrer les menaces.

4. Choisir l'interface utilisateur la mieux adaptée pour recueillir les signalements

Les sites Web et les centres d'appels sont les deux interfaces les plus courantes pour recueillir et traiter les signalements. Il est déjà possible de signaler des abus via des modules complémentaires (add-on) installés dans les navigateurs ou à partir d'applications mobiles, mais cette pratique n'est pas encore très répandue.

Le choix de l'interface dépendra de paramètres tels que l'organisation locale, le budget ou les compétences disponibles. L'expérience de la majorité des plates-formes étudiées montre qu'elles démarrent souvent avec une petite équipe et un budget limité, puis augmente progressivement leurs capacités, en coopérant notamment avec le secteur privé et public.

5. Rationalisation et partage des résultats

Comme l'a révélé l'étude, les mécanismes de signalement en matière de cybercriminalité contribuent de manière significative à améliorer la coopération entre les services répressifs et à rationaliser les opérations. Ainsi, au moment de mettre en place un mécanisme de signalement, il est capital de définir la manière dont l'information recueillie sera diffusée auprès des services et des autorités, ce qui évitera les chevauchements au niveau des activités et renforcera l'efficacité de l'organisation globale de la police.