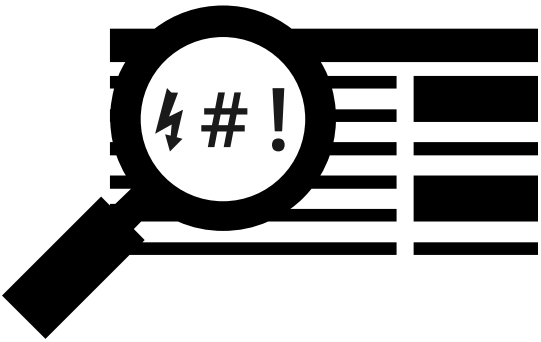
LIVRE BLANC

Contenus illicites en ligne : de la détection au retrait



SOMMAIRE

À nos lectrices et lecteurs,

Ce guide s'adresse à toute personne, rompue à la technique ou pas, connaissant les ressorts juridiques ou profane qui souhaite découvrir ou approfondir la question des responsabilités des acteurs et prestataires techniques sur internet.

Que vous travailliez dans une direction juridique et soyez confronté(e) quotidiennement à des atteintes aux droits de marque détenus par votre entreprise, ou que vous soyez dirigeant d'une PME ne sachant pas vers qui vous tourner pour demander le retrait de certains contenus portant atteinte à vos affaires.

Que vous soyez Policier ou Gendarme et souhaitiez avoir une vision plus claire des différents professionnels avec qui vous travaillez dans le cadre d'une enquête, que vous soyez avocat et souhaitiez actionner le bon interlocuteur, ce livre blanc est fait pour vous.

Il a aussi pour objectif de porter un éclairage sur le travail invisible et souvent méconnu des professionnels qui sont au contact permanent de la criminalité en ligne.

Nous espérons l'avoir réalisé de la manière la plus claire et la plus rigoureuse possible.

EDITO

> ***« Internet reste un refuge pour les délinquants. »*** - phrase d'accroche de l'article « La France mal armée pour enquêter sur le Net » par Fabrice Amedeo paru le 25/04/2011 in lefigaro.fr

Le portail gouvernemental de l'économie indique, pour 2014, que 5,5% du PIB découlent des activités numériques.

Depuis maintenant deux décennies, internet se voit alternativement affublé de deux masques.

L'un, aux traits tordus, où internet serait le lieu où se commettent l'essentiel des délits et crimes de notre monde moderne, leurs auteurs jouissant d'une impunité que personne ne saurait accepter eu égard aux règles qui fondent toute République.

L'autre, aux traits hilares, lorsque bon nombre de spectateurs s'accordent sans mal pour prophétiser que le numérique est une chance, une opportunité à saisir et porteur de moult promesses de croissance économique.

Il n'en reste pas moins que le mythe d'une cybercriminalité galopante dans un internet assimilé au far west, a durablement marqué les esprits. Ces vingt dernières années ont pourtant vu la justice s'adapter, se doter de pôles judiciaires dédiés aux infractions commises en ligne ou via des services en ligne. Ces pôles sont eux-mêmes alimentés par des

services de Gendarmerie et de Police de plus en plus formés et spécialisés dans le traitement de ces infractions spécifiques, à l'instar de l'OCLCTIC ou de la BEFTI.

Cette vision anxiogène guide encore trop de projets législatifs du XXIe siècle déclarant pudiquement un objectif de « meilleure régulation » ou de « sécurisation » des citoyens contre les innombrables tentatives d'escroqueries dont ils seraient les cibles.

De ces tentatives, sous forme de décrets d'exception, d'amendements législatifs qualifiés de « cavaliers » ou d'autorités parajudiciaires aux pouvoirs étendus, résulte un empilement de mesures à l'harmonie douteuse menant, plus ou moins par erreur, à un contrôle des activités, à une surveillance simplifiée des personnes ou à la restriction de libertés, qu'elles soient civiles ou économiques.

En réalité, loin de la zone de non-droit dépeinte ici, « internet », au sens large des activités qui s'y déroulent et de celles qui en dépendent (Quelle entreprise n'envoie aujourd'hui aucun e-mail et n'utilise aucun site web ?), repose à l'heure actuelle sur un large éventail de professions et d'expertises qui, ensemble, concourent à son fonctionnement.

Prompts à agir pour faire cesser les actes illicites ou pour prêter concours à la poursuite de ces faits, ces acteurs ont néanmoins des domaines de compétences et des pouvoirs définis et limités.

De la connaissance des pouvoirs et responsabilités de chaque acteur vis-à-vis d'un contenu illicite dépend l'efficacité de la lutte contre ces contenus et leurs auteurs.

Partis du constat d'un manque de connaissances de nombreuses personnes les interrogeant quotidiennement, à titre personnel ou dans un cadre professionnel, les auteurs de ce livre blanc entendent humblement contribuer à la bonne identification d'un interlocuteur pour obtenir le retrait d'un contenu jugé illicite.

C'est donc au travers de cas d'espèces inspirés ou directement tirés de la réalité que nous vous invitons à découvrir ou à consolider vos connaissances sur le rôle de chaque intermédiaire technique dans la chaîne de publication et de retrait de contenus illicites en ligne.

Certains de ces cas ont fait l'objet d'un atelier dédié au Forum International de la Cybersécurité, le mardi 20 janvier 2015, au Grand Palais de Lille. Ce livre blanc reprend les scénarios évoqués lors de cet atelier et des nouveaux scénarios qui n'y ont pas été évoqués.

Vous pouvez retrouver l'ensemble de la présentation effectuée ce jour-là sur http://pres.gandi.net

1. PHISHING

Contextualisation :

Après avoir reçu un e-mail émanant de « contact@ma-super-banque.fr », j'ai cliqué sur le lien qu'il contenait pour me connecter à mon espace et lire le message. J'ai eu un souci pour me connecter, j'ai décidé de lire le message plus tard. Depuis, je remarque des retraits dont je ne suis pas l'auteur sur mon compte bancaire.

 **REGISTRE [AFNIC]**	« Signalement à l'OCLCTIC » « Vérification du titulaire du nom de domaine litigieux »
 **FAI**	« Signaler : Abuse & FAI » « Pédagogie » « Listes noires navigateur » « Fermeture des sites »
 **REGISTRAR & HÉBERGEUR**	« Suspension domaine » « Coupure serveur »
 **CERT**	« Détection » « Notification aux FAI / Registrar / Hébergeur » « Surveillance »
 **FORCES DE L'ORDRE**	« Récupérer les données chez l'hébergeur (logs, kit) » « Prévenir les tiers si ce n'est déjà fait »

2. MALWARE

Contextualisation :

J'édite un site de presse en ligne et un CERT a averti ma DSI d'une infection visant la section « Bourse & Cotation » en particulier. Après vérification, il s'avère que toutes les personnes qui ont visualisé cette section ont vu leur terminal potentiellement infecté.

	**HÉBERGEUR**	« Signalement » « Pédagogie »
	**CERT**	« Détection et analyse » « Notification aux propriétaires / Hébergeur(s) / Registrar / listes noires » « Surveillance »
	**FORCES DE L'ORDRE**	« Récupérer les données en ligne et chez l'hébergeur » « Identifier les victimes potentielles » « Prévenir les tiers si ce n'est déjà fait »

3. SPAM

Contextualisation :

Depuis que j'ai passé commande sur un site de e-commerce, je reçois de nombreux messages et offres promotionnelles malgré ma désinscription de la liste de diffusion.

	**FAI**	« Signaler comme indésirable » « Dialogue » « Blocage »
	**REGISTRAR**	« Signalement » « Rappel de la loi » « Menace suspension »
	**FORCES DE L'ORDRE**	« Vérifier auprès de Signal Spam l'ampleur de la campagne » « Identifier les acteurs concernés (annonceur, routeur de messagerie, gestionnaire de liste) » « Ouvrir une enquête le cas échéant »

4. FRAUDE 419 / SCAM DIT « À LA NIGÉRIANE »

Contextualisation :

J'ai reçu un message émanant d'un inconnu sur mon adresse personnelle : il semblerait qu'une personne riche, héritière d'un gouvernant déchu en Afrique, ait besoin de mon aide pour encaisser une forte somme dont elle partagera une part.

 **FAI**	« Adresses IP et adresses e-mail émettant le message étiquetées ”spammeur” » « Si compte Orange, blocage du compte émettant et retour vers client usurpé. »
 **FORCES DE L'ORDRE**	« Si préjudice (versement de sommes, escroquerie) réception de la plainte. » « Recueil des en-têtes de courriels auprès de la victime » « Si adresse tierce piratée pour envoyer les messages frauduleux : recueil de la plainte de la victime du piratage initial avec informations (listes des IP ayant accédé à la messagerie) »

5. DÉFIGURATION DE SITE

Contextualisation :

Je viens de me rendre sur le site que j'ai créé pour ma famille. Au lieu des photos de notre dernier voyage, une page noire avec des drapeaux à têtes de mort apparaît et une mention « HaCkEd By Rev0LUt1oN cYb3r ArmY ».

 **CERT**	« Identifier la source de la défiguration » « Préserver les données qui pourraient devenir des preuves » « Identifier la ou les vulnérabilité(s) exploitée(s) » « Evaluer l'étendue des dégâts » « Nettoyer, corriger et reconstruire »
 **HÉBERGEUR**	« Aide à la remise en ligne du site » « Correction des failles éventuelles » « Conseil pour dépôt de plainte »
 **FORCES DE L'ORDRE**	« Réception de la plainte » « Collecte du contenu intégral du site web modifié » « Préservation des journaux de connexion, journaux Apache ou applicatifs (CMS, ...) » « Journaux de connexion sur le compte d'administration de l'hébergement »

6. CONTENUS INCITANT À LA HAINE RACIALE

Contextualisation :

Je travaille au département juridique d'un hébergeur. On m'envoie un e-mail au sujet d'un blog que nous hébergeons. Après consultation du blog, il s'avère que les pages développent un long argumentaire sur l'infériorité de certaines « races humaines » par rapport à d'autres.

 **REGISTRE [AFNIC]**	« Réglementation excluant l'intervention directe. » « Procédure SYRELI (L. 45-2-1 Code Postes et Communications Electroniques) : atteinte ordre public, droits garantis par la Constitution ou la loi pouvant mener à la suppression du nom de domaine »
 **HÉBERGEUR**	« Notification à PHAROS » « Après leur validation, suspension (pas de destruction des contenus) »
 **FORCES DE L'ORDRE**	« Recherche de preuves : copies écran, contenus dépubliés mais si possible non-supprimés » « Réception et traitement plainte »

7. DIFFAMATION

Contextualisation :

Je viens de faire une recherche de mon nom sur un moteur de recherche. Le premier résultat est un site où il est écrit « Cette femme est une voleuse et un escroc : j'ai la preuve qu'elle s'offre des bouteilles de champagne avec l'argent de sa société. »

 **HÉBERGEUR**	« Pas d'intervention sur contenus, transmission de la demande à l'éditeur du site si celui-ci est un particulier, renvoi vers mentions légales si professionnel »
 **FORCES DE L'ORDRE**	« Si inconnu : plainte simple (éventuellement avec constitution de partie civile) » « Réception de la plainte et décision du Parquet pour poursuite des investigations » « Si personne connue : contacter avocat et citation directe contre auteur dénommé »

GLOSSAIRE

Comme tout milieu professionnel, internet s'appuie sur un jargon particulier et utilise force acronymes et sigles.

En voici un aperçu non exhaustif, loin s'en faut, avec leur définition et quelques explications pour vous permettre d'approfondir les problématiques évoquées dans ce livre blanc.

ABUSE

Service et équipe dédiée, chez un hébergeur ou un Registrar, au traitement de plaintes relatives à l'utilisation qui est faite des services fournis par le professionnel. Les plaintes émanent de tiers ou des clients directement.

BEFTI

Brigade d'Enquête sur les Fraudes aux Technologies de l'Information.

CERT

Computer Emergency Response Team. Organisations privées assurant, pour le compte de leur client/employeur, un rôle de prévention des risques et de traitement des menaces et incidents informatiques.

CONTENUS « MANIFESTEMENT ILLICITES »

Catégorie particulière de contenus publiés sur internet bénéficiant d'un régime à part. Il s'agit, de manière exclusive, de contenus constituant une apologie de crime contre l'humanité, pédopornographiques, incitant à la haine raciale et, depuis la

promulgation de la loi 2014-873 pour l'égalité réelle entre les femmes et les hommes, des contenus incitant à la haine à l'égard de personnes à raison de leur sexe, de leur orientation ou identité sexuelle ou de leur handicap.

Voir aussi : **LCEN**

DSI

Direction des Systèmes d'Information.

FAI

Fournisseur d'Accès à Internet.

LCEN

Loi n°2004-575 du 21 juin 2004 modifiée, dite « *Loi pour la confiance dans l'économie numérique* ».

Transposition, dans la législation française, de la directive 2000/31/CE du 8 juin 2000 « relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur ("directive sur le commerce électronique") », cette loi établit le régime juridique de nombreux prestataires de services en ligne qui ne sont responsables du non-retrait de contenus qu'une fois établie leur connaissance effective de ces contenus et de leur caractère illicite.

OCLCTIC

Office Central de Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication.

PHISHING

(se prononce comme « fishing ») : escroquerie type sur internet visant à faire croire à la victime qu'elle est en contact avec un interlocuteur légitime, que ce soit par voie de messagerie ou

directement sur un site web, par exemple. L'objectif étant que la personne trompée fournisse à son insu des informations confidentielles (identifiants et codes d'accès notamment).

REGISTRE

Autorité de tutelle d'une extension (voir aussi : TLD) établissant les règles d'éligibilité et assurant la centralisation des enregistrements de noms de domaine de cette extension.

Exemple : l'Association Française pour le Nommage Internet en Coopération pour l'extension .FR.

REGISTRAR

Prestataire technique assurant l'enregistrement de noms de domaine dans différentes extensions directement auprès du Registre, pour le compte de ses clients.

Le Registrar n'est pas nécessairement l'hébergeur du site web qui pourrait être associé au nom de domaine.

SERVEUR

Équipement réseau traitant des requêtes de la part de « clients » notamment utilisé pour mettre à disposition des contenus sur internet (serveur d'hébergement).

SCAM

Mot anglais signifiant « arnaque », « fraude ». Généralement un message électronique constituant ou participant à une escroquerie, notamment en prêtant à son auteur une qualité qu'il n'a pas (responsable d'une société, représentant d'une banque, affilié à un gouvernement...).

SPAM

Communications non sollicitées envoyées automatiquement, parfois de manière répétée, à un grand nombre de destinataires.

On distingue parfois deux types de spam : ceux envoyés dans un objectif commercial (démarchage) et ceux envoyés dans un but frauduleux (vente de médicaments en ligne par une officine non autorisée ou même par une fausse officine, vente de contrefaçons).

Voir aussi : **Scam**

SITE WEB

Ensemble de pages et ressources mises à disposition via un serveur d'hébergement. Consultées, le plus souvent, depuis un navigateur web.

TLD

Top-Level Domain, extension en français.

Exemple : .FR (extension nationale ou « Country Code TLD ») ou .COM (extension générique, ou « Generic TLD »).

URL

Uniform Resource Locator, il s'agit d'une adresse complète pointant directement vers une page web ou un contenu de celle-ci (image, son...).

REMERCIEMENTS

Nous tenons à remercier l'ensemble des personnes, sociétés, associations et autorités publiques qui ont participé, tant à la réalisation de l'atelier « Contenus illicites : de la détection au retrait » qui s'est déroulé au Forum International de la Cybersécurité le 20 janvier 2015, qu'à la rédaction de ce livre blanc.

Pour leur expertise, leurs corrections, leurs suggestions et leur disponibilité, nous remercions Madame Isabel TOUTAUD (**AFNIC**), Monsieur Alain DOUSTALET (**Orange**), Monsieur Jean-Philippe TEISSIER (**CERT Société Générale**), Monsieur Eric FREYSSINET (**Gendarmerie Nationale**), Monsieur Stéphane BORTZMEYER (**AFNIC**), Monsieur Miroslav KURDOV et Messieurs Alexandre HUGLA et Charles–Edouard PEZÉ (**GANDI.NET**).

Vous pouvez consulter et imprimer de nouvelles copies de ce livre blanc en vous rendant à l'adresse suivante :
http://pres.gandi.net