A Monsieur le Procureur de la République près le Tribunal de Grande Instance de Paris

PLAINTE

POUR :

1. **La Fédération Internationale des Ligues des Droits de l'Homme,** Organisation internationale non gouvernementale, ayant statut consultatif auprès des Nations Unies, de l'UNESCO et du Conseil de l'Europe, et d'observateur auprès de la Commission africaine des Droits de l'Homme et des Peuples,
Déclarée en France conformément à la loi de 1901 sur les associations, ayant pour objet la défense des droits de l'Homme, conformément aux principes inscrits dans la Déclaration Universelle des Droits de l'Homme de 1948,
Dont le siège social est 17, Passage de la Main d'Or – 75011 Paris,
Représentée par son Président, Monsieur Karim Lahidji, domicilié en cette qualité audit siège.

[ci-après « **FIDH** »]

Ayant pour Avocats :

Maître Patrick Baudouin
19, avenue Rapp. 75007 PARIS
Tel. : 01 45 55 86 37 - 01 45 55 45 44
Fax : 01 45 55 88 72

Maître Emmanuel Daoud
9 bis rue Boissy d'Anglas 75008 PARIS
Tel. : 01 55 27 93 93
Fax : 01 55 27 93 94

Chez lesquels il est élu domicile

2. **La Ligue française pour la défense des droits de l'Homme et du Citoyen**, déclarée conformément à la loi de 1901 sur les associations, ayant son siège social à Paris 17018, 138, rue Marcadet, poursuite et diligences de son Président, M. Pierre TARTAKOWSKY, élisant domicile au dit siège et encore en l'étude de ses avocats :

<u>Ayant pour avocat</u> :

Maître Michel TUBIANA
19, rue d'Anjou 75008 PARIS

Maître Jacques MONTACIE de la SCP HUVELIN & Associés
19, rue d'Anjou 75008 PARIS
Tel : 01.53.53.04.80 / Fax : 01.42.25.50.28

Chez lesquels il est élu domicile

[ci-après « **LDH** »]

<u>CONTRE</u> : **X**

Ont l'honneur de déposer plainte contre **X,** des chefs d'infraction de :

- **Accès et maintien frauduleux dans tout ou partie d'un système de traitement automatisé de données** (article 323-1 du code pénal) ;
- **Collecte de données à caractère personnel par un moyen frauduleux, déloyal ou illicite** (article 226-18 du code pénal) ;
- **Atteinte volontaire à l'intimité de la vie privée d'autrui** (article 226-1 du code pénal) ;
- **Utilisation et conservation d'enregistrements et de documents obtenus par le moyen d'une atteinte à l'intimité de la vie privée d'autrui** (article 226-2 du code pénal) ;
- **Atteinte au secret des correspondances électroniques** (article 226-15 alinéa 2 du code pénal)

ET ONT L'HONNEUR DE VOUS EXPOSER LES FAITS SUIVANTS

I – RAPPEL DES FAITS

1. M. Edward Snowden, ex-technicien de la CIA, ayant travaillé à la NSA pendant 4 ans, est à l'origine d'une divulgation de documents faisant état de l'existence d'un programme américain collectant des renseignements sur les serveurs de différentes sociétés exerçant dans le domaine de l'Internet. Ce programme dénommé PRISM (*Planning Tool for Ressource Intégration Synchronization, and Management)* a été créé sous la présidence de George W. Bush.

Le 7 juin 2013, *The Guardian*, quotidien britannique et *The Washington Post*, quotidien américain, ont publié deux articles relatifs aux documents fournis par M. Edward Snowden.

Un nouveau document fourni par l'ex-technicien de la CIA a donné lieu à un article du journal allemand *Der Spiegel*, lundi 1er juillet 2013.

2. Ces documents classés « secret défense » révèlent que la National Security Agency (ci-après « **NSA** ») et le Federal Bureau of Investigation (ci-après « **FBI** ») disposent d'un accès direct aux serveurs de neuf sociétés américaines exerçant dans le domaine de l'Internet, soit **Microsoft** (depuis 2007), **Yahoo** (depuis 2008), **Google**, **Paltalk** et **Facebook** (depuis 2009), **Youtube** et **Skype** (depuis 2010), **AOL** (depuis 2011) et enfin **Apple** (depuis 2012).

Le programme PRISM leur permet de collecter des données matérielles hébergées par les serveurs de ces sociétés incluant notamment les historiques de recherches et de connexions effectuées sur le net, le contenu d'emails, de communications audio et vidéos, des fichiers photos, des transferts de documents ainsi que le contenu de conversations en ligne.

Cette collecte de données s'opère uniquement sur le trafic d'informations effectué à ou vers l'étranger et directement sur les serveurs des sociétés concernées.

Il s'agit d'une surveillance électronique de masse pratiquée par la NSA et le FBI. Tel que l'explique M. Edward SNOWDEN : « *La NSA a construit une infrastructure qui lui permet d'intercepter pratiquement tout* » (pièce n°1 : « *Ed Snowden, le lanceur d'alerte qui défie Barack Obama* » Le Monde, 10 juin 2013)

Il précise par ailleurs : « *Mais d'une manière générale, la réalité est la suivante : si la NSA, le FBI, la CIA, le DIA [Defence Intelligence Agency] et d'autres veulent interroger des bases de données brutes de renseignement électronique, ils peuvent 'entrer' et obtenir ce qu'ils veulent. Numéros de téléphones, mails, identifiants, numéro unique d'un téléphone portable [numéro IMEI]... Tout ça, c'est pareil. Les restrictions portées à cet accès sont de nature politiques, et non techniques ; elles peuvent changer à tout moment »* (Pièce n°2 : « Edward Snowden : "Le FBI, la NSA et la CIA peuvent obtenir tout ce qu'ils veulent" », Le Monde, 17 juin 2013)

Ainsi, à raison d'un demi-milliard de communications privées surveillées par mois (pièce n°3 : « *Surveillance, comment des Etats-Unis espionnent leurs* alliés » Der Spiegel, 1er juillet 2013), selon les documents recueillis, la NSA a déjà collecté plus de 97 milliards d'informations en mars 2013 (pièce n°4 : **«** *Comprendre le programme "Prism"*» Le Monde, 11 juin 2013).

3. A cet égard, les sociétés susvisées ont formellement démenti non seulement avoir eu connaissance de ce programme mais aussi avoir fourni un accès à leurs serveurs.

A titre d'exemple, Steve Dowling, porte-parole d'Apple, soutient n'avoir jamais entendu parler de PRISM ou fourni aux agences du gouvernement un accès direct aux serveurs de la société. Toute agence du gouvernement souhaitant obtenir des données hébergées dans les serveurs, doit nécessairement apporter la preuve d'une décision judiciaire (pièce n°5 :« *U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program* » The Washington Post, 7 juin 2013)

4. Pourtant l'administration américaine affirme que le programme PRISM était déjà connu depuis 2006. A ce titre, le Président Obama précise : *« Ce que nous avons ce sont deux programmes qui ont d'abord été autorisés par le Congrès et encore autorisés par le Congrès »*.

De plus, des experts estiment que les sociétés concernées ne pouvaient ignorer la collecte des données matérielles hébergées sur leurs serveurs et auraient même été tenues de mettre en place les moyens techniques nécessaires pour permettre cette collecte (pièce n°6 : « *Derrière l'antiterrorisme, l'espionnage industriel* » Le Monde, 2 juillet 2013)

Le directeur des renseignements américains a, quant à lui, publié un communiqué dans lequel il affirme que : *« Nous ne pouvons cibler des personnes étrangères sans des objectifs valides de renseignements étrangers »* et ajoute que le programme PRISM est supervisé par un tribunal *«composé de 11 juges désignés par le président de la Cour Suprême des États-Unis »*.

*

Il résulte des éléments divulgués par la presse que les U.S.A ont mis en place un système d'interception des données privées qui concerne tout autant les citoyens américains que les associations et individus étrangers.

L'essence même de ce système est, notamment au travers de mots clés, d'appréhender non seulement l'origine d'un message privé mais aussi son destinataire ainsi que son contenu, quel que soit le moyen technique utilisé pour la transmission de ce message.

Ces faits conduisent à penser que, sous couvert de lutte contre le terrorisme et la criminalité organisée, le gouvernement des U.S.A s'affranchit des règles de la territorialité pour créer un système de contrôle mondial, hors de toutes garanties légales et à leur seul profit.

C'est dans ces circonstances que, par la présente, les associations soussignées se voient contraintes de porter plainte auprès de Monsieur le Procureur de la République près le Tribunal de grande instance de Paris, afin qu'il soit informé sur les faits sus-mentionnés, susceptibles de recevoir une qualification pénale.

Dans ces conditions, il est indispensable et nécessaire qu'une information judiciaire, ou à tout le moins une enquête préliminaire soit diligentée, afin de caractériser les infractions dénoncées.

II- DISCUSSION

II.1 SUR LA RECEVABILITE DE LA FIDH ET DE LA LDH COMME PARTIES CIVILES

- ***En droit***

L'article 2 alinéa 1er du code de procédure pénale dispose :

> « *L'action civile en réparation du dommage causé par un crime, un délit ou une contravention appartient à tous ceux qui ont personnellement souffert du dommage directement causé par l'infraction.* »

En application de ce texte et au visa notamment des articles 6 de la Convention européenne des droits de l'homme et 3 et 85 du code de procédure pénale, la Cour de cassation, dans son arrêt du 9 novembre 2010, a dégagé le principe général selon lequel :

> « *Pour qu'une constitution de partie civile soit recevable devant la juridiction d'instruction, il suffit que les circonstances sur lesquelles elle s'appuie permettent au juge d'admettre comme possible l'existence du préjudice allégué et la relation directe de celui-ci avec une infraction à la loi pénale.* » (Cass. crim., 9 novembre 2010, n°09-88.272)

En l'espèce, la Cour de cassation a accueilli, tel que l'avait fait le Juge d'instruction, la constitution de partie civile d'une association de lutte contre la corruption pour le détournement de fonds publics, abus de biens sociaux, blanchiment, complicité de ces délits, abus de confiance et recel dès lors que :

> « *Les faits dénoncés, en ce qu'ils concernent la présence en France de biens pouvant provenir de détournements de fonds publics, correspondent aux actions menées par cette association, qui, engageant toutes ses ressources dans cette activité, subit un préjudice personnel, économique, directement causé par les infractions en cause, lesquelles portent* ***atteinte aux intérêts collectifs qu'elle défend et constituent le fondement même de son action ; qu'il a déclaré la constitution de partie civile recevable*** »

La Chambre criminelle rappelle ainsi que les associations sont soumises au régime juridique de droit commun de la constitution de partie civile sans considération, *a priori*, de l'objet de l'association ni de la nature des poursuites.

- ***En l'espèce***

LA FIDH

Les articles 1 et 3 des statuts de la FIDH, association régulièrement déclarée, disposent :

> « *Il est constitué une fédération d'associations destinée à défendre et à mettre en œuvre les principes énoncés dans la Déclaration Universelle des Droits de l'Homme de 1948.*
>
> *[…]*

Elle lutte en faveur du respect des libertés individuelles en matière de traitement des données informatisées *et contre toute atteinte à la dignité, l'intégrité, l'égalité et à la liberté du genre Humain pouvant résulter de l'usage de techniques médicales ou biologiques.* » (gras rajouté par nos soins) (pièce n°7 : Statuts de la FIDH).

LA LDH

Les articles 1 et 3 des statuts de la **LDH** disposent que :

> *« **Elle lutte en faveur du respect des libertés individuelles en matière de traitements des données informatisée**s, et contre toute atteinte à la dignité, à l'intégrité et à la liberté du genre humain pouvant notamment résulter de l'usage des techniques médicales… » .*
>
> *[…]*
>
> *« Ses moyens d'action sont : l'appel à la conscience publique, **les interventions auprès des pouvoirs publics, auprès de toute juridiction, notamment la constitution de partie civile lorsque des personnes sont victimes d'atteintes aux principes ci-dessus visés** et d'actes arbitraires ou de violences de la part des agents de l'Etat. »* (Pièce n°8 : Statuts de la LDH).

Les faits visés par la présente plainte portent sur plusieurs infractions en matière d'accès et de maintien dans un système de traitement automatisé de données et de protection des données personnelles détenues par plusieurs sociétés américaines.

Dès lors, **la FIDH et la LDH**, particulièrement actives dans le domaine du respect de la vie privée et de la lutte contre les abus informatiques, subissent un préjudice personnel et direct causé par les infractions en cause, lesquels portent atteinte aux intérêts collectifs qu'elles défendent et constituent le fondement de leur action.

De plus **la LDH et la FIDH** subissent un préjudice personnel qui résulte du système même d'interception mis en œuvre. Il y a tout lieu de croire, en effet qu'elles ont été l'objet de telles interceptions compte tenu de la nature de leurs activités, notamment lorsqu'elles ont tenté à plusieurs reprises de mettre en cause la responsabilité pénale de dirigeants des Etats-Unis à plusieurs reprises que ce soit sur le territoire français ou aux Etats-Unis même en collaboration avec la ligue américaine de la FIDH, le Center for Constitutional Right (CCR).

On notera à cet égard que la FIDH, la LDH et le CCR avaient déposé à Paris le 25 octobre 2007 une plainte visant Monsieur Donald RUMSFELD, ancien Secrétaire d'état à la Défense (Pièce n°11 : Plainte de la FIDH, la LDH et le CCR)

Il en résulte que **la FIDH et la LDH** sont donc recevables et bien fondées à se constituer partie civile.

II.2 SUR LA COMPETENCE DES JURIDICTIONS FRANÇAISES

- ***En droit***

L'article 113-7 du code pénal dispose que la loi pénale française est applicable à tout crime, ainsi qu'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.

- ***En l'espèce***

Les faits dénoncés concernent l'accès et le maintien frauduleux dans des serveurs de sociétés américaines pour y collecter des données personnelles recueillies à l'étranger, et notamment en France, sur des personnes physiques et morales étrangères.

A cet égard, le document fourni par Edward Snowden au journal allemand *Der Spiegel*, aurait révélé la mise sous surveillance quotidienne de citoyens européens. Il en a résulté l'interception de 15 millions de communications d'internautes en Allemagne et près de 2 millions en France (pièce n°9 : « *Espionnage : Hollande pince les oreilles d'Obama* » Libération, 2 juillet 2013)

Par conséquent, sont directement concernées des personnes physiques et morales françaises, victimes à leur insu de cette collecte frauduleuse de données personnelles.

Ainsi, les faits dénoncés étant constitutifs d'infractions de nature délictuelle, le Ministère public pourra engager des poursuites sur le fondement de la présente plainte (article 113-8 du code pénal).

II.3 SUR LES DIFFERENTES INFRACTIONS

A la lumière de ce qui précède, il apparaît que les éléments factuels décrits sont constitutifs de plusieurs infractions imputables d'une part à la NSA et au FBI comme auteurs principaux et d'autre part aux sociétés précitées comme d'éventuels complices :

- Infraction relative à l'accès et au maintien frauduleux dans tout ou partie d'un système de traitement automatisé de données en application de l'article 323-1 du code pénal (**II.3.1**) ;

- Infraction relative à la collecte frauduleuse de données personnelles en application de l'article 226-18 du code pénal (**II.3.2**).

- Infraction relative à l'atteinte à l'intimité de la vie privée d'autrui en application de l'article 226-1 du code pénal (**II.3.3**) ;

- Infraction relative à l'utilisation et la conservation d'enregistrements et de documents obtenus par le moyen d'une atteinte à l'intimité de la vie privée d'autrui en application de l'article 226-2 du code pénal (**II.3.4**) ;

- Infraction relative à l'atteinte au secret des correspondances électroniques en application de l'article 226-15 alinéa 2 du code pénal (**II.3.5**).

II.3.1 Infraction relative à l'accès et au maintien frauduleux dans tout ou partie d'un système de traitement automatisé

- ***En droit***

L'article 323-1 alinéa 1er du code pénal dispose que :

> « *Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 30000 euros d'amende* »

A ce titre, l'infraction se constitue de :

- **l'élément matériel** : l'accès frauduleux est constitué dès lors qu'une personne non habilitée pénètre dans un système de traitement automatisé de données. Cette introduction frauduleuse doit être réalisée par une personne n'ayant pas le droit d'accéder au système.

  Le maintien peut se traduire par un comportement actif, à savoir que l'auteur utilise les possibilités de traitement du système au-delà de ce qui est autorisé. Il peut également s'agir d'un comportement passif si bien que l'auteur ne fait qu'observer le système de traitement.

- **l'élément moral** : il s'agit d'une infraction intentionnelle. Le délit d'accès et de maintien dans un système de traitement automatisé de données suppose un caractère frauduleux, c'est-à-dire la volonté et la conscience, pour l'agent, de commettre ces actes illicites.

En vertu des dispositions du chapitre 4 de la directive 95/46/CE, reprises par les articles 68, 69 et 70 de la loi informatique et libertés du 6 janvier 1978 modifiée par la loi du 6 août 2004, « *le responsable d'un traitement ne peut transférer des données à caractère personnel vers un Etat n'appartenant pas à la Communauté Européenne que si cet Etat assure un niveau de protection suffisant de la vie privée et des libertés et droits fondamentaux des personnes à l'égard du traitement dont ces données font l'objet ou peuvent faire l'objet*.

Le caractère suffisant du niveau de protection assuré par un Etat, s'apprécie en fonction notamment des dispositions en vigueur dans cet Etat ».

Pour les transferts de données hors des Etats considérés comme pourvus d'une protection suffisante, plusieurs outils juridiques ont été développés pour permettre aux acteurs d'apporter un niveau de protection suffisant, notamment l'adhésion aux principes du « Safe Harbor ».

Ces principes négociés entre les autorités américaines et la Commission européenne en 2001, sont essentiellement basés sur ceux de la directive 95/46 du 24 octobre 1995, précitée.

- ***<u>En l'espèce</u>***

Il résulte des faits précédemment énoncés qu'il y a eu un accès et un maintien frauduleux dans les serveurs des sociétés précitées.

En effet, la NSA et le FBI ont eu accès à des données personnelles hébergées par les serveurs des neuf sociétés américaines susvisées.

Or, en vertu de leurs engagements pris à l'égard des Etats de l'Union européenne, notamment par le biais de leur adhésion au « Safe Harbor », les sociétés devaient assurer un niveau de protection suffisant des données hébergées sur leurs serveurs.

La plupart des sociétés susvisées étaient liées, au moment des faits, par les principes du « Safe Harbor » (Yahoo, Microsoft, Google, Facebook, Apple, AOL).

Ces principes leur imposaient de ne transférer les données à l'Etat américain ou ses agences qu'à la condition que leur législation assure un niveau de protection suffisant. Or, cette condition n'était pas remplie étant donné que le « Foreign Intelligence Surveillance Act Amendement Act » (FISAA) de 2008 autorise toute forme d'espionnage politique et économique à l'encontre des non américains.

Dans ces conditions, les sociétés en question n'ont pas pu légalement autoriser l'accès et le maintien de la NSA et du FBI sur leurs serveurs.

Dès lors, la NSA et le FBI se sont introduits frauduleusement dans les serveurs des sociétés précitées et ce alors même que ces agences savaient pertinemment ne pas en avoir l'autorisation.

En outre, tel qu'il ressort des documents récupérés par le *Washington Post* et le *Guardian*, le maintien de ces deux agences dans les serveurs de ces sociétés ne fait aucun doute.

En effet, il est ainsi précisé qu'en mars 2013, la NSA avait déjà récupéré 97 milliards d'informations. Ces données ont été collectées sur les serveurs de Microsoft depuis 2007, de Yahoo depuis 2008 de Google, Paltalk et Facebook depuis 2009, de Youtube et Skype depuis 2010, d'AOL depuis 2011 et enfin d'Apple depuis 2012. Il en résulte un maintien certain de la NSA et du FBI dans ces serveurs.

En conséquence, il apparait de manière claire que l'infraction d'accès et de maintien frauduleux dans tout ou partie d'un système de traitement automatisé est constituée.

L'article 323-1 alinéa 1er du code pénal permet alors d'engager la responsabilité pénale de celui qui s'est introduit et maintenu frauduleusement dans un système informatique.

En l'espèce, les principaux responsables sont la NSA et le FBI.

En vertu de l'article 121-7 du code pénal, est complice d'un crime ou d'un délit la personne qui, sciemment, par aide ou assistance, en a facilité la préparation ou la consommation.

En l'espèce, les sociétés concernées ont pu mettre en place les moyens techniques nécessaires pour permettre l'accès à leurs serveurs par les agences américaines.

Par ce moyen, les sociétés ont pu permettre ou faciliter la consommation de l'infraction prévue par l'article 323-1 du Code pénal et donc en être les complices.

II.3.2 Infraction relative à la collecte frauduleuse de données personnelles

- **En droit**

L'article 226-18 du code pénal dispose :

> « *Le fait de collecter des données à caractère personnel par un moyen frauduleux, déloyal ou illicite est puni de cinq ans d'emprisonnement et de 300 000 Euros d'amende* »

A ce titre, l'infraction se constitue de :

- **l'élément matériel** : il s'agit, à l'occasion de la collecte de données personnelles ayant une forme quelconque (caractères alphanumériques, image, son, etc.), d'utiliser un moyen quelconque au su ou à l'insu de la personne concernée de manière frauduleuse, déloyale ou illicite.

- **l'élément moral** : le délit de l'article 226-18 du code pénal est intentionnel. L'élément moral résulte de la volonté de collecter des données personnelles.

- **En l'espèce**

L'infraction est ici clairement constituée.

La NSA et le FBI ont utilisé le programme PRISM afin de récupérer des données dont le caractère personnel ne peut être remis en cause. En effet, tel que précédemment précisé, il s'agit d'emails, de documents audiovisuels …

Cette collecte d'information apparait comme manifestement frauduleuse, illicite et déloyale.

En effet, tel que précédemment développé, la NSA et le FBI se sont introduits sans aucune autorisation légale dans les serveurs de ces neuf sociétés américaines afin de collecter des données ayant un caractère personnel. Il s'agit donc là d'une collecte dont le caractère frauduleux est évident.

En outre, ces données avaient été légalement hébergées sur les serveurs des sociétés concernées et leur utilisation était donc strictement limitée à ce que les règles d'utilisation des données de chaque société prévoyaient. Aucune de ces sociétés ne prévoyait la collecte des données dans le but de lutter contre le terrorisme et les crimes graves, but expressément poursuivi par les agences à l'origine de la collecte. Les agences ne pouvaient donc pas ignorer que ces données n'avaient pas été transmises aux sociétés dans ce but.

Preuve en est, Keith Alexander, chef de la NSA, a ainsi déclaré que les révélations du programme PRISM ont causé « *des dégâts irréversibles et importants à notre pays* », de nature à « *nuire à nous*

et à nos alliés » (pièce n°10 : « *La NSA et le FBI défendent Prism* » Le Monde, 19 juin 2013). Cette déclaration traduit ostensiblement la volonté de la NSA et du FBI de collecter à l'insu des personnes concernées un certain nombre d'informations.

En conséquence, il apparait de manière claire que l'infraction de collecte frauduleuse de données personnelles est constituée.

L'article 226-18 du code pénal permet alors d'engager la responsabilité pénale de celui qui a collecté frauduleusement des données personnelles.

En l'espèce, les principaux responsables sont la NSA et le FBI.

En vertu de l'article 127-1 du code pénal, est complice d'un crime ou d'un délit la personne qui, sciemment, par aide ou assistance, en a facilité la préparation ou la consommation.

En l'espèce, les sociétés concernées ont pu mettre en place les moyens techniques nécessaires pour permettre aux agences américaines de collecter des données directement sur leurs serveurs.

Par ce moyen, les sociétés ont pu permettre ou faciliter la consommation de l'infraction prévue par l'article 226-18 du Code pénal et donc en être les complices.

II.3.3 Infraction relative à l'atteinte volontaire à l'intimité de la vie privée

- **En droit**

L'article 226-1 du code pénal dispose :

> « *Est puni d'un an d'emprisonnement et de 45.000 euros d'amende le fait, au moyen d'un procédé quelconque, volontairement de porter atteinte à l'intimité de la vie privée d'autrui :*
> 1) *En captant, enregistrant ou transmettant, sans le consentement de leur auteur, des paroles prononcées à titre privé ou confidentiel ;*
> 2) *En fixant, enregistrant ou transmettant, sans le consentement de celle-ci, l'image d'une personne se trouvant dans un lieu privé* »

A ce titre, l'infraction se constitue de :

- **l'élément matériel** : il s'agit d'utiliser un moyen quelconque visant à la captation, l'enregistrement et la transmission de la parole et ou de l'image d'une personne, sans son consentement.

- **l'élément moral** : le délit de l'article 226-18 du code pénal est intentionnel. L'élément moral résulte de la volonté d'atteindre à l'intimité de la vie privée d'une personne.

- **En l'espèce**

L'infraction est ici clairement constituée.

En effet, les agences américaines ont, comme il a été démontré plus haut, collecté des données à caractère personnel qui ne leur étaient pas destinées.

Pire, elles ont, selon des experts, exigé des sociétés la mise en place de systèmes permanents afin de scanner toutes leurs données, ce qui constitue un enregistrement des données en question (pièce n°6).

Ces manœuvres ont été effectuées dans le plus grand secret, et donc nécessairement sans le consentement des personnes sur lesquelles portent ces données

La volonté des agences d'atteindre à la vie privée des personnes découle du caractère intrinsèquement personnel des données collectées.

En l'espèce, les principaux responsables sont le NSA et le FBI.

En vertu de l'article 127-1 du code pénal, est complice d'un crime ou d'un délit la personne qui, sciemment, par aide ou assistance, en a facilité la préparation ou la consommation.

En l'espèce, les sociétés concernées ont pu mettre en place les moyens techniques nécessaires pour permettre la collecte par les agences américaines, sur leurs serveurs, de données qui ont trait à l'intimité de la vie privée des personnes.

Par ce moyen, les sociétés ont pu permettre ou faciliter la consommation de l'infraction prévue par l'article 226-1 du Code pénal et donc en être les complices.

II.3.4 Infraction relative à l'utilisation et la conservation d'enregistrements et de documents obtenus par le moyen d'une atteinte à l'intimité de la vie privée d'autrui

- **En droit**

L'article 226-2 du code pénal dispose :

> *« Est puni des mêmes peines [que l'article 226-1] le fait de conserver, porter ou laisser porter à la connaissance du public ou d'un tiers ou d'utiliser de quelque manière que ce soit tout enregistrement ou document à l'aide d'un des actes prévus par l'article 226-1 »*

- **En l'espèce**

L'infraction est ici clairement constituée.

En effet, les agences américaines ne se sont pas contentées de collecter automatiquement des données auprès des Sociétés, elles les ont en outre remises entre les mains d'analystes afin d'être utilisées dans un but déterminé, la lutte contre le terrorisme.

En l'espèce, les principaux responsables sont le NSA et le FBI.

En vertu de l'article 127-1 du code pénal, est complice d'un crime ou d'un délit la personne qui, sciemment, par aide ou assistance, en a facilité la préparation ou la consommation.

En l'espèce, les sociétés concernées ont pu mettre en place les moyens techniques nécessaires pour permettre l'utilisation de données portant atteinte à l'intimité de la vie privée.

Par ce moyen, les sociétés ont pu permettre ou faciliter la consommation de l'infraction prévue par l'article 226-2 du Code pénal et donc en être les complices.

II.3.3 Infraction relative à l'atteinte au secret des correspondances

- **En droit**

L'article 226-15 al 2 du code pénal dispose :

> « *Est puni des mêmes peines [1 an d'emprisonnement et 45 000 Euros d'amende] le fait, commis de mauvaise foi, d'intercepter, de détourner, d'utiliser ou de divulguer des correspondances émises, transmises ou reçues par la voie électronique ».*

A ce titre, l'infraction se constitue de :

- **l'élément matériel** : Il s'agit de la prise de connaissance ou de l'utilisation du contenu d'une correspondance électronique par une personne à qui elle n'était pas adressée.

- **l'élément moral** : Le délit de l'article 226-15 al 2 du code pénal est intentionnel. L'élément moral résulte de la connaissance par la personne à l'origine de l'atteinte de ce que les correspondances ne lui étaient pas destinées.

- **En l'espèce**

Parmi les données collectées et traitées par les agences américaines, figuraient des communications d'internautes constituant des correspondances et protégées ainsi par le secret.

Les agences ne pouvaient ignorer que les échanges concernés ne leurs étaient pas adressés.

En l'espèce, les principaux responsables sont le NSA et le FBI.

En vertu de l'article 127-1 du code pénal, est complice d'un crime ou d'un délit la personne qui, sciemment, par aide ou assistance, en a facilité la préparation ou la consommation.

En l'espèce, les sociétés concernées ont pu mettre en place les moyens techniques permettant aux agences américaines d'accéder au contenu des correspondances des internautes.

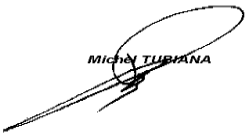
Par ce moyen, les sociétés ont pu permettre ou faciliter la consommation de l'infraction prévue par l'article 226-15 al 2 du Code pénal et donc en être les complices.

*

* *

EN CONSEQUENCE, eu égard à l'ensemble des éléments exposés, la FIDH et la LDH sont valablement fondées à déposer plainte contre X entre les mains de Monsieur le Procureur de la République du Tribunal de Grande Instance de Paris pour les faits visés à la présente plainte et/ou pour tout autre fait que pourrait révéler l'enquête préliminaire ou l'instruction qui serait confiée au Magistrat-Instructeur désigné.

Fait à Paris, le 11 juillet 2013.



PATRICK BAUDOUIN **EMMANUEL DAOUD** **Jacques MONTACIE** **MICHEL TUBIANA**

Annexe 1
Liste des pièces à l'appui :

- Pièce n°1 : « *Ed snowden, le « lanceur d'alerte » qui défie Barack Obama* » Le monde, 10 juin 2013
- Pièce n°2 : « *Edward Snowden : "Le FBI, la NSA et la CIA peuvent obtenir tout ce qu'ils veulent*" » Le Monde 17 juin 2013
- Pièce n°3 : « *Surveillance, comment des Etats-Unis espionnent leurs* alliés » Der Spiegel, 1er juillet 2013
- Pièce n°4 : « *Comprendre le programme "Prism"* » Le Monde, 11 juin 2013
- Pièce n°5 : « *U.S., Bristish intelligence mining data from nine U.S. Internet companies in broad secret program* » The Washington Post, 7 juin 2013
- Pièce n°6 : « *Derrière l'antiterrorisme, l'espionnage industriel* » Le Monde, 2 juillet 2013
- Pièce n°7 : Statuts de la FIDH
- Pièce n°8 : Statuts de la LDH
- Pièce n°9 : « *Espionnage : Hollande pince les oreilles d'Obama* » Libération, 2 juillet 2013
- Pièce n°10 : « *La NSA et le FBI défendent Prism* » Le Monde, 19 juin 2013
- Pièce n°11 : Plainte déposée par la FIDH, la LDH et le CCR le 25 octobre 2007