La FIDH – Fédération internationale des droits de l'Homme – et la LDH – Ligue française des droits de l'Homme – ont saisi le 11 juillet 2013 le Procureur de la République près le Tribunal de Grande Instance de Paris d'une plainte contre X en raison des faits révélés par Edward Snowden.

Agissant tant en raison de leur objet social, qui les conduit à faire sanctionner les atteintes aux libertés individuelles en matière de traitement informatisé, qu'à titre personnel, la FIDH et la LDH ont déposé plainte sur le fondement de certains articles du Code Pénal qui sanctionnent l'accès frauduleux à un système informatisé, la collecte de données à caractère personnel par un moyen frauduleux, l'atteinte volontaire à la vie privée et l'utilisation et la conservation d'enregistrements et de documents obtenus par l'atteinte à la vie privée.

Les révélations faites dans la presse par Monsieur Edward Snowden ont permis de dévoiler l'existence du programme américain dénommé PRISM qui sous couvert de la lutte contre le terrorisme et la criminalité organisée intercepte des données privées, qui concerne tout autant les citoyens américains que les associations et individus étrangers, et a permis à la NSA et au FBI de collecter des données matérielles hébergées par les serveurs de sociétés intervenant sur le net.

L'essence même de ce système – donnant lieu à la surveillance d'un demi-milliard de communications par mois – 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.

Cette intrusion sans contrôle dans la vie de chacun constitue un danger considérable pour les libertés individuelles qui doit être enrayé sous peine de mettre en cause gravement l'Etat de droit. La FIDH et la LDH saisissent donc la justice française afin qu'une information judiciaire portant sur ces faits soit ouverte. Il convient de dire que le parquet a jugé que cette plainte était recevable. Nous attendons avec intérêt les procédures d'instruction concernant des entités dont la puissance pouvait apparaître comme parfaitement protectrice et dissuasive. La FIDH et la LDH ont considéré que la puissance des uns n'impliquait pas l'impuissance des autres et que ce combat méritait d'être mené.

L'argumentation que nous avons présentée a consisté à rappeler l'existence pénale des infractions sur lesquelles se fonder, établir la matérialité des faits, définir ensuite les raisons des associations à se porter en justice, rappeler les compétences à juger des juridictions françaises et enfin à détailler les infractions commises justiciables des articles du code pénal. Je suivrai ce plan pour présenter mon propos.

1) Sur la matérialité des faits

Les documents recueillis ont été classés «secret défense» et révèlent que la National Security Agency et le Federal Bureau of Investigation 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 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». 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 ».

Ainsi, à raison d'un demi-milliard de communications privées surveillées par mois selon les documents recueillis, la NSA a déjà collecté plus de 97 milliards d'informations en mars 2013 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.

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. 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 Etats-Unis 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 les associations se voient contraintes de porter plainte auprès du 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 et pour qu'une information judiciaire, ou à tout le moins une enquête préliminaire soit diligentée, afin de caractériser les infractions dénoncées.

2) Sur la recevabilité de la plainte et la constitution de parties civiles

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, à priori, de l'objet de l'association ni de la nature des poursuites.

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 Rights (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. Il en résulte que la FIDH et la LDH sont donc recevables et bien fondées à se constituer partie civiles.

3) Sur la compétences des juridictions françaises

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. 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. 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 surle fondement de la présente plainte (article 113-8 du code pénal).

4) Sur les différentes infractions

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 et parfaitement identifiées par le code pénal français :

1) **l'accès et le maintien frauduleux dans tout ou partie d'un système de traitement automatisé de données**

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

2) **la collecte frauduleuse de données personnelles ;**

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 apparaît 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 ainsidéclaré 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 ».

3) **l'atteinte à l'intimité de la vie privée d'autrui**

Une autre infraction est constituée par la responsabilité pénale de celui qui a collecté frauduleusement des données personnelles. En l'espèce, les principaux responsables sont la NSA et le FBI. Et les complices sont ceux qui, sciemment, par aide ou assistance, en ont 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.

4) **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**

L'infraction relative à l'atteinte volontaire à l'intimité de la vie privée 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. 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 et les sociétés concernées qui ont mis 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 doivent donc être considérées comme complices.

5) **l'atteinte au secret des correspondances électroniques**

L'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 est 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 avec la complicité active des sociétés concernées offrant leurs services et compétences techniques. Cette infraction relative à l'atteinte au secret des correspondances parachève cet édifice dit technique d'illégalités. 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 conclusion, ce sont bien la NSA et le FBI qui sont les principaux responsables avec la complicité des sociétés qui ont proposé leurs moyens techniques permettant aux agences américaines d'accéder au contenu des correspondances des internautes, aux métadonnées, aux carnets d'adresses, aux flux de messages. C'est ce qui fondent la légitimité de la plainte que nous avons déposée. Tous les défenseurs des droits suivront avec intérêt les suites que donneront les magistrats instructeurs afin qu'elles servent une jurisprudence positive ou servir d'exemple sous d'autres systèmes juridiques.