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
Tél. : 01 45 55 86 37 - 01 45 55 45 44
Fax : 01 45 55 88 72

Maître Emmanuel Daoud
9 rue Boissy d'Anglas 75008 PARIS
Tél. : 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 75018, 138, rue Marcadet, poursuite et diligences de son Président, M. Pierre TARTAKOWSKY, domicilié en cette qualité audit siège .**

Ayant pour avocats :

Maître Michel TUBIANA
19, rue d'Anjou 75008 PARIS

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

Chez lesquels il est élu domicile

[ci-après « LDH »]

CONTRE : X

Ont l'honneur de déposer plainte entre vos mains contre X, des chefs d'infraction suivants :

- 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 8 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales et 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 8 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, article 226-15 alinéa 2 du code pénal et article L241-1 du Code de la sécurité intérieure)
- Recel (article 321-1 du Code pénal)

ET ONT L'HONNEUR DE VOUS EXPOSER LES FAITS SUIVANTS

I – RAPPEL DES FAITS

1. Le 4 juillet, le journal *Le Monde* a révélé qu'un système permettant aux services secrets français de collecter en masse et de manière systématique des signaux électromagnétiques émis par les téléphones et ordinateurs existe également en France (pièce n°1 : « *Révélations sur le big brother français* » Le Monde.fr, 4 juillet 2013).

Bien que ces éléments aient été réfutés par le premier ministre et n'aient pas suscité de réaction de la part du ministère de la Défense (pièce n°2 : « Big Brother français : Matignon défend la légalité du dispositif» Le Monde, 6 juillet 2013), le journal affirme que la direction générale de la sécurité extérieure (DGSE) stocke des données à caractère personnel dans des « *supercalculateurs* ».

Il s'agit ainsi de collecter notamment des mails, sms, relevés d'appels téléphoniques, accès à Facebook, Twitter et d'autres sites internet de particuliers.

Ces données seraient ensuite stockées pendant des années et mutualisées avec les six autres services de renseignement français : la direction centrale du renseignement intérieur (DCRI), la direction nationale du renseignement et des enquêtes douanières (DNRED), la direction de la protection et de la sécurité de la défense (DPSD), la direction du renseignement militaire (DRM), le traitement du renseignement et action contre les circuits financiers clandestins (TRACFIN) et les services du renseignement de la préfecture de police de Paris.

A cet égard, le rapport du 30 avril 2013 rendu par les huit députés et sénateurs membres de la délégation parlementaire aux renseignements indique que « *depuis 2008 des progrès ont été réalisés en matière de mutualisation des capacités, notamment en ce qui concerne le renseignement d'origine électromagnétique, opéré par la DGSE au profit de l'ensemble de la communauté du renseignement* ». Les parlementaires envisageaient alors « *de renforcer les capacités exploitées par la DGSE* » et de « *consolider l'accès des autres services aux capacités mutualisées de la DGSE* » (pièce n°3 : Rapport n°557 de M. Jean-Pierre SUEUR, sénateur et Mme Patricia Adam, députée fait au nom de la délégation parlementaire au renseignement du 30 avril 2013).

2. De plus, Le Monde révèle dans le même dossier (pièce n°4 : « *Quand la police judiciaire utilise des données de la DGSE* » Le Monde.fr, 5 juillet 2013), l'existence de liens directs entre la DGSE et la direction centrale de la police judiciaire. Ainsi, les enquêteurs solliciteraient les moyens de la DGSE dans le domaine du terrorisme, des enquêtes criminelles menées à l'étranger ou dans des affaires de pédophilie.

Les données obtenues en dehors de tout cadre légal, entreraient alors souvent dans la procédure judiciaire sous la forme de renseignements anonymes.

3. Ces informations révélées dans l'article du *Monde* ont été à la fois nuancées et précisées par les publications suivantes et notamment un article paru le 11 juillet sur un blog affilié au journal et un article du Nouvel Observateur en date d'avril 2001, publié à nouveau le 4 juillet 2013 (pièce n°5 : « *La DGSE a le « droit » d'espionner ton Wi-Fi, ton GSM et ton GPS aussi* », bugbrother.blog.lemonde.fr, 11 juillet 2013 et Pièce n°6 : « *La DGSE écoute le monde (et les français) depuis plus de trente ans* », Le Nouvel Observateur, 4 juillet 2013).

Ainsi, ces vingt dernières années, la France a mis en place un réseau mondial d'interceptions. L'article du Nouvel Observateur révèle en effet l'existence de plusieurs bases et antennes d'interception satellitaires rattachées à la DGSE. La première base d'interception se situe dans la forêt guyanaise, au cœur du centre spatial de Kourou, la seconde sur l'île de Mayotte et la troisième dans la banlieue Ouest de Paris, sur le plateau d'Orgeval, aux Alluets-Le-Roi. A ces bases principales, s'ajoutent une trentaine d'antennes satellitaires permettant de couvrir la quasi-totalité du globe (pièce n°6 : « *La DGSE écoute le monde (et les français) depuis plus de trente ans* », Le Nouvel Observateur, 4 juillet 2013).

4. Par ailleurs, des liens étroits existeraient entre la DGSE et la NSA (Agence de sécurité nationale) américaine. En effet, la presse allemande a révélé, grâce à une note d'Edward Snowden, l'existence d'un accord de coopération sur la surveillance entre la France et les Etats-Unis en matière de renseignement connu sous le nom de « Lustre ». La DGSE aurait en effet, selon les informations recueillies par Le Monde, établi un protocole d'échange de données avec les Etats-Unis à partir de la fin 2011 et début 2012 (pièce n°7: « Surveillance : la DGSE a transmis des données à la NSA américaine », Le Monde, 31 octobre 2013).

De même, un haut responsable du renseignement en France a confirmé que la DGSE a adopté fin 2011 un protocole d'échange de données massif avec la NSA (pièce n°8 : « Paris, précieux partenaire de l'espionnage de la NSA », Le Monde, 30 novembre 2013.)

Il apparait que la France bénéficie d'un positionnement stratégique en matière de transport de données électroniques dans la mesure où les câbles sous-marins par lesquels transitent la plupart des données provenant d'Afrique et d'Afghanistan atterrissent à Marseille et en Bretagne.

Pour les agences de renseignement, ce type d'écoutes permet de collecter de très importantes quantités de méta données, c'est-à-dire non seulement le contenu d'une conversation, mais, par exemple, sa date, son lieu et ses participants. C'est ce type de données que la DGSE fournirait à l'Agence nationale de sécurité américaine (pièce n°9 : « La France au cœur de la surveillance des câbles sous-marins de communication », Le Monde, 30 novembre 2013.)

En effet, parmi les documents auxquels Le Monde a eu accès, une première note du 6 août 2007, émanant de la direction de la NSA chargée du renseignement par transmissions électroniques indique que la relation avec la DGSE est « entrée dans une nouvelle dimension ». Désormais, les échanges portent non seulement sur les données techniques mais aussi sur le renseignement possédé par chacun des services. Le niveau de coopération est tel qu'aujourd'hui des données personnelles venant d'Afrique ou du Moyen-Orient, transitant par la France et appartenant à des individus de nationalité française (hommes d'affaires, diplomates, voire à des agents de la DGSE en mission, ou même à des chefs d'Etat africain) peuvent tomber entre les mains de la NSA au nom de l'antiterrorisme (pièce n°8, précitée).

En outre, Le Monde a révélé que, selon un document interne des services secrets britanniques (la GCHQ), la DGSE entretiendrait une coopération étroite avec un opérateur de télécommunication français. L'ancienneté de leurs liens, la description des savoir-faire spécifiques de l'entreprise ainsi que l'enquête du journal Le Monde, ont permis au quotidien de conclure qu'il s'agirait de France Télécom-Orange.

L'une des forces de la DGSE résiderait dans le fait qu'elle ne se contente pas des autorisations accordées par le législateur pour accéder aux données des clients de France Télécom-Orange. Elle

dispose surtout, à l'insu de tout contrôle, d'un accès libre et total à ses réseaux et aux flux de données qui y transitent.

Le président-directeur-général d'Orange, Stéphane Richard, a indiqué que « des personnes habilitées secret-défense peuvent avoir à gérer, au sein de l'entreprise, la relation avec les services de l'Etat et notamment leur accès au réseau mais elles n'ont pas à m'en référer. Tout ceci se fait sous la responsabilité des pouvoirs publics, dans un cadre légal » (pièce n°10 : « Espionnage : comment Orange et les services secrets coopèrent », Le Monde, 20 mars 2014.)

Enfin, dans un article intitulé « interceptions : ce que disent les documents du monde », publié par Le Monde (pièce n°11 : « Que dit le document sur la surveillance téléphonique de la NSA en France», Le Monde, 30 octobre 2013), le quotidien affirme que le document étayant une partie des révélations est un graphique extrait des données soustraites à la NSA par Edward Snowden, que Le Monde a pu consulter grâce au partenariat noué avec le journaliste Glenn Greenwald. Il est issu d'un logiciel, *Boundless Informant*, qui agrège et organise les données entreposées dans les bases de données de la NSA. C'est ainsi que Le Monde a pu avancer le chiffre de 70,3 millions de données téléphoniques collectées concernant la France et incorporées dans les bases de données de l'agence entre le 10 décembre 2012 et le 8 janvier 2013. Le document pourrait contenir à la fois le fruit de la surveillance de la DGSE et les données interceptées par la NSA en France.

* * *

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 susmentionnés, susceptibles de recevoir une qualification pénale.

Force est de constater qu'à ce jour seule une quantité limitée d'informations a été révélée concernant ce programme de surveillance. Ces informations proviennent essentiellement d'enquêtes diligentées par les journalistes du *Monde* et du *Nouvel Observateur* et, dans une moindre mesure, d'un rapport du 30 avril 2013 rendu par les huit députés et sénateurs membres de la délégation parlementaire aux renseignements. Il y a lieu de souligner et de regretter à cet égard les très nombreux passages de ce rapport rendus inaccessibles par leur classement « secret défense ».

Dès lors, il apparait difficile en dehors de toute information judiciaire, ou à tout le moins d'une enquête, d'obtenir davantage d'informations relatives aux faits susvisés.

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, 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)

Dans cet arrêt, 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 aux régimes juridiques 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***

L'article premier des statuts de la FIDH dispose:

« 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'abus des nouvelles technologies ou de l'usage de techniques médicales ou biologiques. »
(Pièce n°12- Les statuts de la FIDH)

De même, les articles 1 et 3 des statuts de la LDH, association régulièrement déclarée, disposent que :

« Elle lutte en faveur du respect des libertés individuelles en matière de traitements des données informatisées, 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°13 : Statuts de la LDH.

En l'espèce, les faits visés par la plainte, en ce qu'ils concernent plusieurs infractions en matière d'accès et de maintien dans un système de traitement automatisé de données et de protection des données personnelles, correspondent aux actions menées par la FIDH et la LDH qui, engageant des ressources non négligeable dans cette activité, subissent un préjudice personnel, économique, directement causé par les infractions en cause, lesquelles portent atteinte aux intérêts collectifs qu'elles défendend et constituent le fondement même de son action.

En outre, il convient de souligner que la FIDH et la LDH sont intervenues dans le débat public au moment de la discussion au Sénat, puis de la promulgation, le 18 décembre 2013, de la loi n° 2013-1168 dite « loi de programmation militaire ». Ce texte a introduit des changements substantiels dans les procédures de recueil et de conservation des données numériques par les agences de renseignement françaises. La loi a ainsi accru les possibilités de collecte et de traitement des données sans contrôle judiciaire (pièce n°14 – « Loi de programmation militaire : le scandale qui fait sploutch, Rue89/Nouvel Obs, le 19 décembre 2013), ce que la FIDH et la LDH ont dénoncé en appelant les sénateurs à amender le projet de loi (pièce n°15 – « France : le projet de loi de programmation militaire doit être amendé », site internet de la FIDH, 6 décembre 2013).

La FIDH et la LDH ont toutes deux adressé aux parlementaires une lettre ouverte afin d'inciter à une saisine du Conseil constitutionnel, après l'adoption de cette loi (pièce n°16 - Lettre ouverte du 13 décembre 2013).

L'implication de la FIDH et de la LDH dans le débat public au regard de la collecte et du traitement de données par les services de renseignements est donc indéniable.

Il en résulte que la FIDH et la LDH sont recevables et bien fondées à déposer la présente plainte.

II.2 SUR LA VIOLATION DE LA CONVENTION EUROPEENNE DE SAUVEGARDE DES DROITS DE L'HOMME ET DES LIBERTES FONDAMENTALES (CESDH).

- **En droit,**

L'article 8 de la CESDH dispose que :

« 1. Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance.

2. Il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui. »

La Cour européenne des droits de l'Homme considère la simple mémorisation des données relatives à la vie privée d'un individu comme une ingérence au sens de l'article 8 de la Convention (CEDH *Leander c. Suède*, 26 mars 1987 ; *Kopp c. Suisse*, 25 mars 1998 et *Amann c. Suisse*, 16 février 2000).

Elle a récemment rappelé que *« la protection des données à caractère personnel joue un rôle fondamental pour l'exercice du droit au respect de la vie privée et familiale consacré par l'article 8 de la Convention. La législation interne doit donc ménager des garanties appropriées pour empêcher toute utilisation de données à caractère personnel qui ne serait pas conforme aux garanties prévues dans cet article »* (CEDH Brunet c/ France, 18 septembre 2014).

En conséquence, la juridiction considère que *« pour ne pas enfreindre l'article 8 cette ingérence doit avoir été prévue par la loi, poursuivre un but légitime au regard du paragraphe 2 et, de surcroît, être nécessaire dans une société démocratique pour atteindre ce but »* (CEDH *Rotaru c. Roumanie*, 4 mai 2000).

- <u>En l'espèce,</u>

Les faits relatés par le journal *Le Monde* dans son édition du 4 juillet 2013 impliquent une mémorisation de données relatives à la vie privée de plusieurs individus et constituent une ingérence dans le droit au respect de la vie privée des personnes visées.

- <u>Cette ingérence n'est pas prévue par la loi</u> :

  - ❖ En effet, il ne pourra être considéré que les faits de collecte de données à caractère personnel se sont déroulés dans le cadre de la loi n°91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des communications électroniques. Les dispositions légales susvisées prévoient seulement des autorisations à titre exceptionnel d'interceptions de correspondances émises par voie électronique, dans un but déterminé (article L 241-2 du Code de la sécurité intérieure), par des personnels habilités (article L 242-1 du Code la sécurité intérieure) et pour une durée maximum de quatre mois (article L 242-3 du Code de la sécurité intérieure). Or, l'enquête du journal *Le Monde* relate un stockage massif de données techniques par les services secrets qui n'est en rien défini, et *a fortiori* autorisé par cette législation. Cette collecte de masse se fait de façon systématique et automatique, en dehors de toute procédure légale, et vise à conserver les données concernées sans limite temporelle.

    L'article 20 de la loi de 1991 précitée, aujourd'hui intégré au code de la sécurité intérieure à l'article L 241-3 prévoit certes un régime dérogatoire lorsque la collecte des données est faite dans le cadre de la défense des intérêts nationaux :

« Les mesures prises par les pouvoirs publics pour assurer, aux seules fins de défense des intérêts nationaux, la surveillance et le contrôle des transmissions empruntant la voie hertzienne ne sont pas soumises aux dispositions des titres Ier et II de la présente loi ».

Même en présence de cette réserve, le dispositif ne pourra être considéré comme étant respectueux du droit européen des droits de l'Homme. Cette disposition légale ne satisfait pas aux exigences de qualité de la loi imposées par la Cour européenne, à deux égards.

En effet :

- d'une part, cette disposition a pour seul objet de soustraire du régime de garanties relatives à la protection des données personnelles, les atteintes effectuées au nom de la défense des intérêts de la Nation, sans que lui soit substitué un autre régime juridique, même plus souple.
  Or, si La Cour européenne a déjà eu l'occasion d'affirmer le caractère légitime de la lutte contre le terrorisme (décision CEDH *Klass et autres c. Allemagne*, 6 septembre 1978, §42), elle n'en considère pas moins que les actes effectués dans le cadre de la poursuite de ce but légitime doivent être entourés d'un certain nombre de garanties essentielles. Ainsi, la Cour européenne des droits de l'homme a, de longue date, considéré que *« si l'article 8 a essentiellement pour objet de prémunir l'individu contre les ingérences arbitraires des pouvoirs publics, il ne se contente pas de commander à l'Etat de s'abstenir de pareilles ingérences : à cet engagement plutôt négatif peuvent s'ajouter des obligations positives inhérentes à un respect effectif de la vie privée et familiales »* (CEDH 26 mars 1985, *X. et Y. c/Pays-Bas §23).*
  En particulier, dans une affaire relative au système roumain de collecte et d'archivage d'informations, elle a conclu que l'absence de contrôle prévu dans la loi démontrait *«que le droit interne n'indique pas avec assez de clarté l'étendue et les modalités d'exercice du pouvoir d'appréciation des autorités dans le domaine considéré ».* La Cour en a conclu que *« la détention et l'utilisation par le SRI d'information sur la vie privée du requérant n'étaient pas « prévues par la loi », ce qui suffit à constituer une méconnaissance de l'article 8 » (CEDH 26 mars 1987, Leander c/ Suède §§67).*
  Au surplus, dans ce même arrêt, la Cour européenne a considéré que l'absence de procédure de contrôle dans la loi l'empêche de vérifier la légitimité du but recherché par les mesures ordonnées et *« si celles-ci étaient, à supposer le but légitime, « nécessaire dans une société démocratique ».*

- d'autre part, cette disposition vise uniquement le spectre hertzien, imposé par la Cour. Cependant, aujourd'hui, le spectre hertzien sert en matière de radio-identification, de GPS, de GSM et de Wi-Fi... technologies dont l'utilisation par le grand public est bien plus banalisée de nos jours qu'en 1991. Partant, cette dérogation à toute forme de contrôle, prévue en 1991 afin de *« ne pas enfermer* [le service secret] *dans son quota d'écoutes autorisées »* témoigne de l'obsolescence des prescriptions légales encadrant les interceptions de communications et partant, du non-respect du principe de proportionnalité entre le but poursuivi et les moyens employés tel que l'impose la CEDH.

- Cette collecte massive n'est pas non plus prévue par le décret n°91-1052 du 14 octobre 1991 relatif au fichier informatisé du terrorisme mis en œuvre par les services des renseignements généraux du ministère de l'intérieur. En effet, si ce décret prévoit la mise en œuvre d'un fichier informatisé par les services susvisés, celui-ci a pour finalité exclusive de « *centraliser des informations qui concernent les personnes qui peuvent, en raison de leur activité individuelle ou collective, porter atteinte à la sûreté de l'Etat ou à la sécurité publique par le recours actif apporté à la violence, ainsi que les personnes entretenant ou ayant entretenu des relations directes et non fortuites avec celles-ci* » (article 2 du décret du 14 octobre 1991). Ce décret définit précisément en son article 3 les informations à caractère personnel pouvant faire l'objet d'un traitement automatisé. Les correspondances personnelles ne figurent pas parmi ces informations. Enfin, ce décret prévoit un contrôle quinquennal du fichier par la Commission nationale informatique et libertés (CNIL) qui n'a jamais eu lieu sur le fichier dont il est fait état dans la présente plainte.

Les faits objets de la plainte sont donc dépourvus de base légale.

Au surplus,

- <u>Cette ingérence ne poursuit pas un but légitime.</u>

  - La Cour européenne a déjà eu l'occasion d'affirmer le caractère légitime de la lutte contre le terrorisme (« *les sociétés démocratiques se trouvent menacées de nos jours par des formes très complexes d'espionnage et par le terrorisme, de sorte que l'Etat doit être capable, pour combattre efficacement ces menaces, de surveiller en secret les éléments subversifs opérant sur son territoire* » décision CEDH *Klass et autres c. Allemagne*, 6 septembre 1978, §42).
    Pour autant, l'Etat français a eu recours à l'espionnage des citoyens sans se limiter aux seuls domaines du terrorisme et de la défense du patrimoine économique. L'énoncé très flou de la « *protection de la sécurité nationale* » permet de viser un nombre très important et surtout indéfini d'individus. Ainsi, le journal *Le Monde* affirme que la police judiciaire a recours au traitement informatisé géré par la DGSE, y puisant quotidiennement les données qui les intéressent, notamment dans le cadre d'enquêtes criminelles de droit commun.

L'interception des communications par la DGSE ne poursuit donc pas un but légitime.

- La Cour européenne soucieuse de ne pas voir « *saper, voire détruite, la démocratie au motif de la défendre, affirme que les Etats ne sauraient prendre, au nom de la lutte contre l'espionnage et le terrorisme n'importe quelle mesure jugée par eux appropriée* » (décision *CEDH Klass et autres c. Allemagne*, 6 septembre 1978, §49), contrôle enfin la proportionnalité des moyens mis en œuvre pour atteindre le but poursuivi. Ces moyens sont disproportionnés en l'espèce. En effet, le traitement capte et enregistre des données de manière automatique, sans « *cible* » prédéterminée, de sorte qu'il vise n'importe quel individu ayant des échanges électromagnétiques en lien avec le territoire français. Ce mode de traitement n'assure donc pas de contrôle relatif au caractère à la fois pertinent et non excessif des données collectées par rapport au but poursuivi comme l'exige la Cour (décisions CEDH *Rotaru c. Roumanie*, 4 mai 2000, *Marper c/ Royaume Uni*, 4 décembre 2008 et *Association « 21 décembre 1989 » et autres c. Roumanie*, 24 mai 2011).

L'interception massive des communications par la DGSE n'est donc ni prévue par la loi, ni proportionnée à un but légitime poursuivi. Cette ingérence n'est donc pas nécessaire dans une société démocratique.

La collecte et l'enregistrement des données à caractère personnel et échanges électromagnétiques effectués par la DGSE constituent donc une violation de l'article 8 de la CEDH.

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 :

- Infraction relative à l'accès et au maintien frauduleux dans tout ou partie d'un système de traitement automatisé de données (II.3.1) ;
- Infraction relative à la collecte frauduleuse de données personnelles (II.3.2).
- Infraction relative à l'atteinte à l'intimité de la vie privée d'autrui (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 (II.3.4) ;
- Infraction relative à l'atteinte au secret des correspondances électroniques (II.3.5) ;
- Infraction relative au recel (II.3.6).

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 l'espèce***

Il résulte des faits précédemment énoncés qu'il y a eu un accès et un maintien frauduleux dans les serveurs des sociétés hébergeant des données à caractère personnel.

En effet, le dossier du journal *Le Monde*, met en exergue le contrôle de la DGSE sur l'identifiant des internautes, le lieu, la date, la durée, le poids des mails échangés. Cette surveillance implique nécessairement un accès et un maintien actif sur les serveurs des sites hébergeant ce type de données tels que Google, Facebook, Microsoft, Apple, Yahoo, etc.

Or cet accès et ce maintien actifs, automatiques et durables sur ces serveurs caractérisent la matérialité de l'infraction susmentionnée.

De plus, le caractère frauduleux est constitué par le contournement du dispositif légal régissant l'accès à ce type de données.

En effet, comme évoqué précédemment, la loi de 1991 pose un cadre juridique strict et contraignant qui interdit notamment le traitement des correspondances émises par la voie de communications électroniques de manière massive et automatique.

En outre, en vertu de la loi dite « Informatique et liberté » du 6 janvier 1978 et du décret du 14 octobre 1991, une démarche de réquisition ou d'interception de données est ciblée et ne peut être réalisée de manière massive, tant quantitativement que temporellement. De telles pratiques ne sont donc pas fondées légalement.

En conséquence, il apparait 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, le principal responsable est le directeur de la DGSE et ses éventuels complices au sein du ministère de la défense.

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

- **En droit**

L'article 226-18 du code pénal dispose que :

« 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.

- **<u>En l'espèce</u>**

L'infraction est ici clairement constituée.

La DGSE emploie une équipe de crypto-mathématiciens qui pénètre les systèmes informatiques et collecte des millions de données dont le caractère personnel ne peut être remis en cause. En effet, il s'agit d'emails, d'identifiants, de sms et de conversations audiovisuelles.

Dès 2010, Bernard BARBIER directeur technique de la DGSE, avait expliqué que les grands réseaux publics étaient « *la cible principal* » et que les services de renseignement stockaient « *tous les mots de passe* ».

Cette collecte d'informations apparaît comme manifestement frauduleuse, illicite et déloyale.

En effet, la DGSE semble s'être introduite, en dehors du cadre légal, dans les serveurs de sociétés de l'internet 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 l'agence à l'origine de la collecte. Les renseignements français ne pouvaient donc pas ignorer que ces données n'avaient pas été transmises aux sociétés dans ce but.

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, le principal responsable est le directeur de la DGSE et ses éventuels complices au sein du ministère de la défense.

<u>II.3.3 Infraction relative à l'atteinte volontaire à l'intimité de la vie privée</u>

- **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, la DGSE a, comme il a été démontré plus avant, collecté des données à caractère personnel qui ne lui étaient pas destinées.

Pire, elle ne s'est pas contentée de collecter des données directement en lien avec le but qu'elle poursuit, elle a procédé à des traitements massifs, sans cibler les personnes pouvant en faire l'objet ni limiter les informations pouvant être collectées.

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'attenter à la vie privée des personnes découle du caractère intrinsèquement personnel des données collectées.

L'article 226-1 du code pénal permet alors d'engager la responsabilité pénale de celui qui a violé la vie privée d'autrui.

En l'espèce, le principal responsable est le directeur de la DGSE et ses éventuels complices au sein du ministère de la défense.

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.

Ainsi la DGSE a mis en place une «*infrastructure de mutualisation* » de ces données en les partageant avec les six autres services de renseignements qui n'en étaient pas plus les destinataires autorisés. Partant, elle a commis une nouvelle infraction, en ce qu'elle a organisé la communication à des tiers des informations collectées en violation de l'intimité de la vie privée.

Par ailleurs, en puisant quotidiennement des informations sensibles au gré de leurs besoins, les autres services de renseignement se sont également rendus responsables de cette violation.

En l'espèce, les principaux responsables sont l'ensemble des services de renseignements français, à savoir : le directeur de la direction centrale du renseignement intérieur (DCRI), le directeur de la direction nationale du renseignement et des enquêtes douanières (DNRED), le directeur de la direction de la protection et de la sécurité de la défense (DPSD), le directeur de la direction du renseignement militaire (DRM), le directeur du traitement du renseignement et action contre les circuits financiers clandestins (TRACFIN) et le directeur des services du renseignement de la préfecture de police de Paris et leurs éventuels complices dans les différents ministères de tutelle.

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.

Du reste, par une décision rendue le 2 novembre 2000, la 17ème chambre du Tribunal correctionnel de Paris est venue éclaircir le statut du courrier électronique en assimilant à l'échange épistolaire. Pour le Tribunal, il ne fait pas de doute que «*le terme " correspondance " désigne toute relation par écrit existant entre deux personnes identifiables, qu'il s'agisse de lettres, de messages ou de plis fermés ou ouverts* » (TCom Paris, 17ème ch., 2 nov. 2000).

- **En l'espèce**

Parmi les données collectées et traitées par la DGSE et les autres services de renseignements, figuraient des communications d'utilisateurs de télécommunications constituant des correspondances et protégées ainsi par le secret.

Ces services ne pouvaient ignorer que les échanges concernés ne leurs étaient pas adressés.

En outre, la jurisprudence considère qu'il y a atteinte au secret des correspondances dès lors que l'interception, la lecture et la retranscription de messages nécessite une dérivation et sont effectuées au moyen d'un artifice ou d'un stratagème (CA Paris, 17 déc. 2001).

Eu égard à la nature et à l'ampleur des interceptions, il est manifeste que la DGSE a eu recourt à une dérivation constituant un artifice ou un stratagème dont il résulte une violation du secret des correspondances.

En l'espèce, les principaux responsables sont l'ensemble des services de renseignements français, à savoir : le directeur de la direction centrale du renseignement intérieur (DCRI), le directeur de la direction nationale du renseignement et des enquêtes douanières (DNRED), le directeur de la direction de la protection et de la sécurité de la défense (DPSD), le directeur de la direction du renseignement militaire (DRM), le directeur du traitement du renseignement et action contre les circuits financiers clandestins (TRACFIN) et le directeur des services du renseignement de la préfecture de police de Paris et leurs éventuels complices dans les différents ministères de tutelle.

II.3.6 Infraction relative au recel de données à caractère personnel

- **En droit**

L'article 321-1 alinéa 2 du code pénal dispose :

> *« Constitue [également] un recel le fait, en connaissance de cause, de bénéficier, par tout moyen, du produit d'un crime ou d'un délit »*

A ce titre, l'infraction se constitue de :

- **l'élément matériel** : Il s'agit de bénéficier, en connaissance de cause, et par un moyen quelconque du produit d'un crime et d'un délit.
  La chose recelée peut-être incorporelle dès lors que l'auteur de l'infraction en a tiré profit.

- **l'élément moral** : Le délit de l'article 321-1 alinéa 2 du code pénal est intentionnel. L'élément moral consiste en la connaissance de l'origine frauduleuse de la chose recelée.

- **<u>En l'espèce</u>**

Les services de renseignement ont bénéficié de données à caractère personnel obtenues frauduleusement par la DGSE.

En effet, comme démontré plus haut, cette dernière a accédé sans autorisation à des serveurs informatiques, y a collecté frauduleusement des données sensibles, violant ainsi à la fois l'intimité de la vie privée et le secret des correspondances des internautes.

Les services de renseignement, en puisant dans l'interface de données mise en place par la DGSE, ont commis un recel de ces quatre infractions.

En l'espèce, les principaux responsables sont l'ensemble des services de renseignements français, à savoir : le directeur de la direction centrale du renseignement intérieur (DCRI), le directeur de la direction nationale du renseignement et des enquêtes douanières (DNRED), le directeur de la direction de la protection et de la sécurité de la défense (DPSD), le directeur de la direction du renseignement militaire (DRM), le directeur du traitement du renseignement et action contre les circuits financiers clandestins (TRACFIN) et le directeur des services du renseignement de la préfecture de police de Paris et leurs éventuels complices dans les différents ministères de tutelle.

*
* *

En conséquence, 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

PATRICK BAUDOUIN EMMANUEL DAOUD Jacques MONTACIE MICHEL TUBIANA

Liste des pièces à l'appui

Pièce n°1 : « Révélations sur le big brother français » Le Monde, 4 juillet 2013
Pièce n°2 : «Big Brother français : Matignon défend la légalité du dispositif», Le Monde, 6 juillet 2013
Pièce n°3 : Rapport n°557 de M. Jean-Pierre SUEUR, sénateur et Mme Patricia Adam, députée fait au nom de la délégation parlementaire au renseignement du 30 avril 2013
Pièce n°4 : « Quand la police judiciaire utilise des données de la DGSE » Le Monde, 5 juillet 2013
Pièce n°5 : « La DGSE a le « droit » d'espionner ton Wi-Fi, ton GSM et ton GPS aussi », bugbrother.blog.lemonde.fr, 11 juillet 2013
Pièce n°6 : « La DGSE écoute le monde (et les français) depuis plus de trente ans », Le Nouvel Observateur, 4 juillet 2013
Pièce n°7 : « Surveillance : la DGSE a transmis des données à la NSA américaine », Le Monde, 31 octobre 2013
Pièce n°8 : « Paris, précieux partenaire de l'espionnage de la NSA », Le Monde, 30 novembre 2013
Pièce n°9 : « La France au cœur de la surveillance des câbles sous-marins de communication », Le Monde, 30 novembre 2013
Pièce n°10 : « Espionnage : comment Orange et les services secrets coopèrent », Le Monde, 20 mars 2014
Pièce n°11 : « Que dit le document sur la surveillance téléphonique de la NSA en France ? », Le Monde, 30 octobre 2013
Pièce n°12 : Statuts de la FIDH
Pièce n°13 : Statuts de la LDH
Pièce n°14 : « Loi de programmation militaire : le scandale qui fait sploutch », Rue89/Nouvel Obs, 19 décembre 2013
Pièce n°15 : « France : le projet de loi de programmation militaire doit être amendé », site internet de la FIDH, 6 décembre 2013
Pièce n°16 : Lettre ouverte de la FIDH et de la LDH du 13 décembre 2013