The Ciric Law Firm, PLLC 17A Stuyvesant Oval, New York, NY 10009

Pierre Ciric, Esq.
Member of the Firm
Ph. 212.260.6090
Fx. 212.529.3647
pciric@ciriclawfirm.com
www.ciriclawfirm.com

Le 22 Septembre 2015

A l'attention de Mme Isabelle Falque-Pierrotin
Conseiller d'État, Présidente
Commission Nationale de l'Informatique et des Libertés
8, rue Vivienne
CS 30223
75083 Paris cedex 02
France
Tél : 01 53 73 22 22
Fax : 01 53 73 22 00
Par courriel : ifalque-pierrotin@cnil.fr

PAR COURRIER ELECTRONIQUE, TELEFAX ET COURRIER

RE : PLAINTE AUPRES DE LA COMMISSION NATIONALE INFORMATIQUE ET LIBERTES RELATIVE A LA MISE EN ŒUVRE DE SYSTEMES DE COLLECTE ET DE TRAITEMENT DE DONNEES A CARACTERE PERSONNEL

Madame la Présidente,

en application des articles 11, 38 et 41 de la Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, dans sa version consolidée au 18 septembre 2015, je vous demande d'enregistrer cette lettre comme plainte relative à la mise en œuvre de systèmes de collecte et de traitements de données à caractère personnel.

1. Rappel des faits

a. Concernant le contexte procédural de la demande :

Aux Etats-Unis, l'avocat enregistré auprès d'un des 50 barreaux américains est soumis à une obligation déontologique sévère consistant à s'assurer de mettre en place « *des mesures raisonnables nécessaires à la représentation de son client* », et d'agir de façon compétente pour

« *sauvegarder l'information relative à la représentation d'un client contre une communication inadvertente ou non autorisée par l'avocat ou toute autre personne qui participe à la représentation du client ou qui sont sujets à la supervision de l'avocat.* » ABA Model Rule 1.1, ABA Model Rule 1.6, Comment 16.

Le 26 Juillet 2015, le magazine « L'OBS » publiait un article intitulé « *INFO OBS. Pourquoi les écoutes de la DGSE sont illégales depuis sept ans* » (disponible sur http://tempsreel.nouvelobs.com/societe/20150726.OBS3205/info-obs-pourquoi-les-ecoutes-de-la-dgse-sont-illegales-depuis-sept-ans.html). Cet article faisait suite à un premier article publié par le même magazine, le 1er juillet 2015, intitulé « *Comment la France écoute aussi le monde* » (http://tempsreel.nouvelobs.com/societe/20150625.OBS1569/exclusif-comment-la-france-ecoute-aussi-le-monde.html). Aux fins de nous assurer de la véracité de ces articles, nous avons demandé une confirmation de la part du magazine « L'OBS » de l'absence de démenti communiqué auprès de ce magazine concernant les informations contenues dans ces articles.

Ces articles révèlent publiquement pour la première fois de façon documentée les points suivants, s'il s'avère que les faits allégués dans ces articles sont exacts :

- La DGSE a mis en place, 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, des écoutes de grande envergure sur certains types de communications entre des parties privées présentes en France et des parties privées présentes aux Etats-Unis concernant les communications transmises sur un câble traitant une communication téléphonique opérée sur une ligne fixe.
- Le Premier Ministre a, en avril 2008, et hors du cadre de la loi suscitée, signé un décret secret et non publié au Journal Officiel de la République Française, autorisant la DGSE à opérer des écoutes de grande envergure sur certains types de communications entre des parties privées présentes en France et des parties privées présentes aux Etats-Unis concernant les communications opérées sur un câble en fibres optiques traitant une communication par courriel, SMS, ou téléphone portable, et ce sans l'autorisation préalable de la CNCIS car traitée pays par pays, et non pas individu par individu. La presse rapporte en effet que la quasi-totalité des communications intercontinentales est désormais transmise par câble sous-marin, et non pas par satellite (voir Maxime Vaudano, *Les câbles sous-marins, clé de voûte de la cyber surveillance*, LE MONDE, 6 septembre 2013, disponible sur http://www.lemonde.fr/technologies/article/2013/08/23/les-cables-sous-marins-cle-de-voute-de-la-cybersurveillance_3465101_651865.html).
- La DGSE a mis en place l'intégralité de ces systèmes d'écoutes autorisés par ce décret secret.

De plus, Patricia Adam, rapporteure de la proposition de loi relative aux mesures de surveillance des communications électroniques internationales, n° 3042, déposée le 9 septembre 2015 a confirmé, a confirmé, durant l'examen du texte au cours de la réunion du 16 septembre

2015 en commission de la défense nationale et des forces armées, l'existence du décret secret d'avril 2008 Voir COMMISSION DE LA DEFENSE : MESURES DE SURVEILLANCE DES COMMUNICATIONS ELECTRONIQUES INTERNATIONALES, Ppl relative aux mesures de surveillance des communications électroniques internationales, Examen des articles, disponible sur http://videos.assemblee-nationale.fr/Datas/an/portail/video.3133584_55f93becd2df3.commission-de-la-defense--mesures-de-surveillance-des-communications-electroniques-internationales-16-septembre-2015).

La French American Bar Association, Inc. (ci-après « FABA »), association d'avocats et juristes franco-américains de premier plan réunissant aux Etats-Unis un grand nombre d'adhérents. Les adhérents de la FABA, dont je suis le Vice-Président, sont admis, soit au barreau français, soit à l'un des 50 barreaux américains, soit à la fois en France et aux Etats-Unis.

La FABA avait, le 14 juillet 2015, soumis des observations au Conseil Constitutionnel dans le cadre de contrôle de constitutionnalité des normes, exprimant des objections motivées contre l'article L.821.7 de la loi (voir Texte Adopté n° 542 à l'Assemblée Nationale, quatorzième Législature, Session Ordinaire de 2014-2015, 24 Juin 2015, Projet de Loi relatif au renseignement, (Texte définitif), disponible sur http://www.assemblee-nationale.fr/14/ta/ta0542.asp). En effet, cet article remettait en cause le secret professionnel protégeant la profession d'avocat et l'obligation de confidentialité des échanges entre l'avocat et son client pour les avocats situés hors du territoire national, et créait également une rupture du principe d'égalité devant les restrictions des libertés publiques entre les avocats localisés sur le territoire national et les avocats localisés hors du territoire national.

Le 26 juillet 2015, dans sa décision n° 2015-713 DC, le Conseil Constitutionnel, bien que préservant l'essentiel de l'article L. 821-7, abondait dans le sens des observations de la FABA, en déclarant l'intégralité de l'article L.854-1 autorisant les écoutes internationales contraire à la Constitution.

Par conséquent, le Conseil Constitutionnel jugeait qu'étaient contraires à la Constitution l'intégralité de la mise en place des pratiques décrites par les articles de presse suscités concernant les écoutes pratiquées entre les parties privées localisées en France et les parties privées localisées aux Etats-Unis, en particulier lorsque l'une des parties privées est un avocat localisé hors de France, et ce entre le 1er avril 2008 au moins et le 26 juillet 2015.

Suite à la publication des articles dans le magazine « L'OBS » en juillet 2015, la FABA, envoyait au Premier Ministre, en vertu des articles L. 821-1 et L. 821-4 de la loi n° 2015-912 du 24 juillet 2015 relative au renseignement, une lettre demandant notamment au Premier Ministre de confirmer que la DGSE a, depuis le 27 juillet 2015, le lendemain de la date de la publication de la décision n° 2015-713 DC au Journal Officiel de la République Française, cessé toute pratique autorisée par le décret secret d'avril 2008, et concernant en particulier les communications entre les avocats membres de la FABA et leurs clients, si au moins l'une des parties est présente en France (voir PJ n°1). A ce jour, ce courrier est resté sans réponse.

b. Concernant les requérants

Je soussigné, Pierre Ciric, suis de nationalité française, et né à Paris, 75, XVIIIe arrondissement. Je suis également de nationalité américaine, et suis domicilié dans l'Etat de New York. Je suis également immatriculé auprès du Consulat Général de France à New York (« Consulat »), localisé au 934 Fifth Avenue, New York, NY 10021.

Je suis également avocat admis au barreau de l'Etat de New York, et partenaire du cabinet «The Ciric Law Firm, PLLC », un cabinet incorporé dans l'Etat de New York sous la forme d'une société à responsabilité limitée (voir PJ n°2).

Durant la période incriminée, du 1er avril 2008 au 24 juillet 2015, période durant laquelle des écoutes de masse ont été effectuées non pas par individu mais par groupe de pays sur la base des méthodes décrites dans les articles indiquées ci-dessus, j'ai effectué de nombreuses communications par téléphone, courrier électronique, textes, SKYPE et autres moyens de nature électronique en tant qu'avocat avec plusieurs clients basés en France aux fins de représenter leurs intérêts devant des juridictions américaines.

Du fait des contraintes de secret professionnel suscitées, je ne puis vous fournir aucun détail concernant les dates, les contenus ou les destinataires de ces communications

Durant la même période, j'ai également effectué de nombreuses communications par téléphone, courrier électronique, textes, SKYPE et autres moyens de nature électronique en tant que requérant avec plusieurs avocats basés en France dans le cadre de plusieurs contentieux ou l'Etat est lui-même le défendeur, et je suis le requérant. Certaines de ces procédures sont toujours en cours devant plusieurs juridictions françaises.

Ces échanges et de ces conversations ont inclus des données personnelles, soit concernant les confrères avec lesquels j'ai échangé des informations, soit concernant les clients de mon cabinet avec lesquels j'ai échangé des informations.

L'exemple le plus typique de ces échanges de données personnelles est constitué par les lettres d'engagement ou lettres de missions échangées entre avocats et clients. Ces lettres, échangées de façon électronique du fait de l'éloignement géographique, contiennent en général des informations relatifs aux noms, adresses de résidence, adresses professionnelles, adresses courriel, et comptes bancaires des destinataires aux fins de confirmer les termes de la relation professionnelle existant entre un avocat et son client.

c. Concernant les données personnelles et leur traitement non autorisé

Les articles inclus en annexe (voir PJ n°3) démontrent que les requérants ont été victimes de mises en œuvre de systèmes de collectes et de traitements de données à caractère personnel non autorisés.

En effet, ces articles, dont aucun n'a été démenti, démontrent que la DGSE, en collaboration avec les opérateurs Alcatel-Lucent et Orange (ci-après dénommés les « défendeurs ») ont installé une infrastructure technique et informatique basée sur deux principaux outils (voir Gilbert Kallenborn, *Supercalculateurs et fibres optiques … Comment la France espionne le Monde*, 01NET.COM, 1er juillet 2015, disponible sur http://www.01net.com/actualites/supercalculateurs-et-fibres-optiques-comment-la-france-espionne-le-monde-659369.html; Vincent Jauvert, *EXCLUSIF. Comment la France écoute (aussi) le monde*, L'OBS, 1er juillet 2015, disponible sur http://tempsreel.nouvelobs.com/societe/20150625.OBS1569/exclusif-comment-la-france-ecoute-aussi-le-monde.html; Vincent Lamigeon, *Comment les Services de Renseignement Français Surveillent Ce Qui Se Dit sur le Net et au Telephone*, CHALLENGE, 20-09-2013, disponible sur http://www.challenges.fr/economie/20130919.CHA4491/la-verite-sur-les-grandes-oreilles-de-la-dgse.html):

- Des stations d'interceptions opérant sur tous les câbles sous-marins (voir Submarine Cable Map, TELEGEOGRAPHY, disponible sur http://www.submarinecablemap.com/), notamment ceux fournis par Alcatel-Lucent, spécialiste des communications optiques ; ces stations regroupent des équipements, notamment des « splitters » dédoublant les fibres du câble sous-marin, et permettant de subdiviser un flux optique en deux branches identiques et permettant la surveillance continue et systématique des transferts de données sur la branche dédoublée ;
- Au moins un ou plusieurs « data centers, » dont l'un d'entre eux "de 100 mètres de long sur 10 de large" dans les Yvelines, près des Alluets-le-Roi (voir Vincent Lamigeon, *Comment les Services de Renseignement Français Surveillent Ce Qui Se Dit sur le Net et au Telephone*, CHALLENGE, 20-09-2013, disponible sur http://www.challenges.fr/economie/20130919.CHA4491/la-verite-sur-les-grandes-oreilles-de-la-dgse.html).

Par conséquent, ces installations et ces centres de traitement de données sont bien des équipements et systèmes informatiques capables d'effectuer des collectes et traitements sur les données du requérant, puisque les câbles sous-marins traitant des communications entre l'Amérique du Nord et la France font bien partie de ce dispositif.

Ces données sont de 2 ordres, appelés communément contenants et contenus :

- Les contenants : Les données personnelles identifiant les requérants (noms, adresses électroniques, etc.) ;

- Le contenus : les données personnelles identifiant en France les individus, personnes, professionnelles et clients avec lesquels le requérants sont en contact par tous les moyens téléphoniques et électroniques identifiés au paragraphe 1.b ci-dessus.

Or, les articles mentionnés ci-dessus confirment bien que les données soumises à ces traitements sont les informations relevant à la fois des contenants et des contenus.

2. Recevabilité de ma demande

a. Conditions de recevabilité :

Les conditions de recevabilité de cette demande sont définies par les articles suivants.

L'article 11 de la Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés prévoit que :

> *[La Commission nationale de l'informatique et des libertés] reçoit les réclamations, pétitions et plaintes relatives à la mise en œuvre des traitements de données à caractère personnel et informe leurs auteurs des suites données à celles-ci.*

De plus, l'article 38 de la Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés indique que :

> *Toute personne physique a le droit de s'opposer, pour des motifs légitimes, à ce que des données à caractère personnel la concernant fassent l'objet d'un traitement.*

Enfin, l'article 41 de la Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés indique que :

> *Par dérogation aux articles 39 et 40, lorsqu'un traitement intéresse la sûreté de l'État, la défense ou la sécurité publique, le droit d'accès s'exerce dans les conditions prévues par le présent article pour l'ensemble des informations qu'il contient.*
>
> *La demande est adressée à la commission qui désigne l'un de ses membres appartenant ou ayant appartenu au Conseil d'État, à la Cour de cassation ou à la Cour*

> *des comptes pour mener les investigations utiles et faire procéder aux modifications nécessaires. Celui-ci peut se faire assister d'un agent de la commission. Il est notifié au requérant qu'il a été procédé aux vérifications.*
>
> *Lorsque la commission constate, en accord avec le responsable du traitement, que la communication des données qui y sont contenues ne met pas en cause ses finalités, la sûreté de l'État, la défense ou la sécurité publique, ces données peuvent être communiquées au requérant.*

Par conséquent, le fait que la collecte et le traitement des données personnelles soit effectué par l'Etat ou par ses agents n'exclut aucunement l'intervention de la CNIL aux fins de traiter la demande des requérants.

b. <u>Recevabilité concernant la mise en œuvre de traitements de données à caractère personnel.</u>

L'article 2 de la Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés spécifie le champ des mises en œuvre de traitements de données à caractère personnel.

> *Constitue une donnée à caractère personnel toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres. Pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accès le responsable du traitement ou toute autre personne.*
>
> *Constitue un traitement de données à caractère personnel toute opération ou tout ensemble d'opérations portant sur de telles données, quel que soit le procédé utilisé, et notamment la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion,*

> *ainsi que le verrouillage, l'effacement ou la destruction.*
>
> *Constitue un fichier de données à caractère personnel tout ensemble structuré et stable de données à caractère personnel accessibles selon des critères déterminés.*
>
> *La personne concernée par un traitement de données à caractère personnel est celle à laquelle se rapportent les données qui font l'objet du traitement.*

Or, les systèmes de collecte et de traitements effectués par les défendeurs et décrits au paragraphe 1.c suscité tombent bien dans la définition de *« traitement de données à caractère personnel »*. En effet, les données personnelles identifiant les requérants ainsi que les données personnelles identifiant en France les individus, personnes, entités professionnelles et clients avec lesquels les requérants sont en contact par tous les moyens téléphoniques et électroniques identifiés ci-dessus tombent bien dans la définition de « *donnée à caractère personnel »*, à savoir toute

> *« opération ou tout ensemble d'opérations portant sur de telles données, quel que soit le procédé utilisé, et notamment la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction. »*

De plus, les communications incriminées ont été l'objet, au moins entre le 1er avril 2008 et le 26 juillet 2015, d'un système d'écoutes systématiques décrites dans les articles ci-dessus.

c. Recevabilité quant à la qualité donnant capacité à agir :

En ce qui concerne Pierre Ciric, tout individu majeur, quel que soit sa nationalité, a la capacité à agir devant la CNIL. Aucune limite de nationalité n'existe. Le fait que le requérant soit de nationalité française n'influence en rien sa capacité à agir. Le fait que le requérant soit domicilié à l'étranger ne représente aucun obstacle à sa capacité d'ester en justice devant la CNIL. Enfin, il n'est frappé d'aucun défaut de capacité. Le requérant, en tant que personne majeure, de plus avocat admis au barreau de New York, a donc la capacité juridique d'agir devant la CNIL.

En ce qui concerne le cabinet « The Ciric Law Firm, PLLC », une société à responsabilité limitée de droit américain, cette société a la capacité juridique, de par son président ou l'un de ses partenaires, de déposer des actions en justice partout où il a la compétence pour le faire.

Cette capacité est établie par le reçu de l'Etat de New York, daté du 27 septembre 2011 (voir PJ n°2).

De plus, le fait que « The Ciric Law Firm, PLLC » soit une société de droit américain ne peut être opposé à sa capacité d'ester en justice devant des juridictions françaises. En effet, l'arrêt « *Ligue du Monde islamique et Organisation islamique mondiale du secours islamique contre France, CEDH, 15/01/2009, Requêtes nos 36497/05 et 37172/05)* » a condamné la France pour les restrictions imposées aux associations étrangères pour ester en justice devant les tribunaux français.

La CEDH a en effet déclaré qu'elle estimait :

> *« qu'en exigeant la déclaration prévue à l'article 5 de la loi de 1901 pour une association étrangère n'ayant pas de " principal établissement " en France et souhaitant introduire une action en diffamation afin de lui permettre d'ester en justice, les autorités françaises n'ont pas seulement sanctionné l'inobservation d'une simple formalité nécessaire à la protection de l'ordre public et des tiers, comme le soutient le gouvernement. Elles ont aussi imposé aux requérantes une véritable restriction, au demeurant non suffisamment prévisible, qui porte atteinte à la substance même de leur droit d'accès à un tribunal, de sorte qu'il y a eu violation de l'article 6 de la Convention ».*
> Ligue du Monde islamique et Organisation islamique mondiale du secours islamique contre France, CEDH, 15/01/2009, *Requêtes nos 36497/05 et 37172/05),* §58.

Par conséquent, le fait que le cabinet « The Ciric Law Firm, PLLC » soit une association de droit américain ne constitue pas une atteinte à sa capacité d'ester en justice devant la CNIL.

d. Recevabilité quant à la qualité donnant intérêt à agir :

i. Concernant le requérant Pierre Ciric

L'article 38 de la Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés confirme que :

Toute personne physique a le droit de s'opposer, pour des motifs légitimes, à ce que des données à caractère personnel la concernant fassent l'objet d'un traitement.

Dans le cadre de la jurisprudence administrative classique, le requérant satisfait à toutes les conditions jurisprudentielles usuelles de l'intérêt à agir, selon lequel tout requérant qui a un intérêt suffisant à l'intervention de la CNIL peut effectuer une demande.

L'intérêt à agir s'apprécie, dans le cadre de la jurisprudence administrative, sur le fait que le requérant qui a un intérêt direct et suffisant à la remise en cause de l'interception qu'il attaque, est recevable à agir.

Cet intérêt peut revêtir trois caractéristiques.

En premier lieu, l'intérêt doit être né et actuel, ainsi que revêtir un certain degré de certitude. La jurisprudence n'exige pas que l'intérêt soit strictement né pour pouvoir agir ; mais, si l'intérêt est futur et certain, alors l'intérêt sera considéré comme né. La jurisprudence admet toutefois l'intérêt éventuel, s'il est hautement probable (*CE, 11 mars 1903, Lot, Rec. Lebon, p. 780*, acceptant comme recevable la requête d'un archiviste paléographe attaquant la décision de nomination d'une personne n'ayant pas cette qualité dans un emploi ordinairement réservé aux archivistes paléographes ; *CE, 14 février 1975, Da Silva, Rec. Lebon, p. 16*, acceptant comme recevable un recours formé par un étranger contre le décret modifiant les conditions de délivrance et de renouvellement des cartes de séjour et de travail).

En deuxième lieu, l'intérêt peut être matériel ou moral, à condition que l'acte fasse grief au requérant (*CE, 8 février 1908, Abbé Deliard, Rec. Lebon, p. 127*, acceptant comme intérêt à agir l'intérêt d'un prêtre au respect de la liberté religieuse ; *CE, 13 juillet 1948, Association des anciens élèves de l'école Polytechnique*, acceptant comme intérêt à agir l'intérêt de l'association à défendre le prestige de l'école).

En troisième lieu, l'intérêt doit être direct et personnel vis-à-vis du requérant, en ce sens que le requérant doit être concerné personnellement par la décision qu'il conteste, parce que son application serait de nature à modifier sa situation juridique.

Dans le cas d'espèce, toutes ces conditions sont largement remplies par les requérants.

Tout d'abord, l'intérêt à agir est né, actuel et certain, au moment de l'enregistrement de cette demande, puisque le préjudice subi par le requérant, c'est-à-dire a) la violation du secret professionnel opéré par les interceptions engagées par les défendeurs et b) la violation des droits de la défense et du principe de l'égalité des armes par l'enregistrement des conversations du requérant avec ses avocats dans le cadre de procédure contre l'Etat, ont été déjà constatées ou sont hautement probables, et ce pour une période extrêmement longue.

L'intérêt à agir satisfait également à la deuxième condition suscitée, puisque l'intérêt du requérant mis en cause est bien matériel, puisqu'il affecte a) la violation du secret professionnel opéré par les interceptions engagées par l'autorité publique et donc la conduite de ses affaires avec ses clients, et b) la violation des droits de la défense et du principe de l'égalité des armes par l'enregistrement des conversations du requérant avec ses avocats dans le cadre de procédures contre l'Etat a affecté directement la capacité du requérant à communiquer en toute confiance avec ses avocats localisés en France.

Enfin, l'intérêt du requérant satisfait à la troisième condition suscitée, dans la mesure où le requérant a un intérêt direct à la préservation la plus absolue du secret professionnel ainsi que de la confidentialité de ses communications avec ses avocats localisés en France.

ii. Concernant le requérant « The Ciric Law Firm, PLLC »

Dans la mesure où « The Ciric Law Firm, PLLC » est une société à responsabilité limitée dont le but est de fournir des services juridiques à ses clients, cette société a également un intérêt à agir significatif dans la mesure où sa mission est remise en cause par la mise en place des techniques de surveillance décrites dans les articles de presse décrits ci-dessus.

Tout d'abord, l'intérêt à agir est né, actuel et certain, au moment de l'enregistrement de cette demande, puisque le préjudice subi par la société, c'est-à-dire la violation du secret professionnel opérée par les interceptions engagées par l'Etat contre les partenaires du cabinet a été déjà constatée ou est hautement probable, et ce pour une période extrêmement longue.

L'intérêt à agir satisfait également à la deuxième condition suscitée, puisque l'intérêt de la société qui est mis en cause est bien matériel, puisqu'il affecte la violation du secret professionnel opéré par les interceptions engagées par l'Etat et donc la conduite des affaires du cabinet avec ses clients.

Enfin, l'intérêt de la société satisfait à la troisième condition suscitée, dans la mesure où le cabinet a un intérêt direct à la préservation la plus absolue du secret professionnel dont doivent bénéficier les clients du cabinet.

e. Recevabilité quant aux délais :

Aucune condition de délais n'est prévue par la Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

f. Recevabilité quant à l'obligation de ministère d'un avocat :

Ni le code de justice administrative, ni la Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, ne prévoient, dans le cadre d'une requête,

l'intervention d'un avocat attitré au barreau de Paris. Par conséquent, la partie requérante est dispensée du ministère obligatoire d'un avocat admis au barreau de Paris devant la CNIL.

3. **La remise en cause par les défendeurs, du fait des techniques de surveillance incriminées entre le 1er avril 2008 et le 27 juillet 2015, entrainant la collecte et le traitement des données personnelles, du secret professionnel protégeant la profession d'avocat et l'obligation de confidentialité des échanges entre l'avocat et son client dans un contexte international représente un grave préjudice que la CNIL se doit d'identifier, pour lequel elle doit formuler un avis et entreprendre les investigations nécessaires.**

    a. Les actions des défendeurs représentent une multitude de violations systématiques du caractère confidentiel des communications entre l'avocat localisé hors du territoire national et son client basé en France, et ce depuis le 1er avril 2008.

L'avocat inscrit au barreau français est soumis à la doctrine du secret professionnel, première garantie des libertés individuelles, qui oblige l'avocat à préserver le contenu de ses discussions, de ses courriers avec ses clients ainsi que les informations dont il a eu connaissance au cours de ses échanges avec l'avocat de l'adversaire. Le secret couvre toutes les confidences que l'avocat a pu recevoir à raison de son état ou de sa profession dans le domaine du conseil ou de la défense devant les juridictions et ce quels qu'en soient les supports, matériels ou immatériels (papier, télécopie, voie électronique). Les correspondances entre avocats sont par nature confidentielles. Enfin, obligation absolue, le justiciable ne peut délivrer l'avocat du respect du secret professionnel.

C'est la Loi no 97-308 du 7 avril 1997 modifiant notamment l'article 66-5 de la loi no 71-1130 du 31 décembre 1971 portant réforme de certaines professions judiciaires et juridiques qui est venue redéfinir les contours du secret professionnel des avocats :

> *- Art. 66-5. - En toutes matières, que ce soit dans le domaine du conseil ou dans celui de la défense, les consultations adressées par un avocat à son client ou destinées à celui-ci, les correspondances échangées entre le client et son avocat, entre l'avocat et ses confrères, les notes d'entretien et, plus généralement, toutes les pièces du dossier sont couvertes par le secret professionnel.*

La violation du secret professionnel est un délit pénal (article 226-13 et 226-14) et un manquement à la règle déontologique, susceptible d'entraîner parallèlement à l'instance pénale, des sanctions disciplinaires.

L'obligation de confidentialité, couverte par la doctrine du secret professionnel, rend tous les échanges écrits et oraux entre avocats par nature confidentiels. Les correspondances entre avocats, quel qu'en soit le support, ne peuvent en aucun cas être saisies ou produites en justice, ni faire l'objet d'une levée de confidentialité.

Ces deux concepts se retrouvent aux Etats-Unis, sans être exactement équivalents, dans la doctrine dite du « attorney-client privilege » (Restatement (Third) of Law Governing Lawyers. § 68. Attorney-Client Privilege, Federal Rule of Evidence 501, General Rule) et dans la doctrine de la confidentialité (ABA Model Rule 1.6).

Par conséquent un avocat admis, auprès d'un barreau français, soit à l'un des 50 barreaux américains, soit à la fois auprès d'un barreau français et d'un barreau américain bénéficie d'une protection très importante des communications entre celui-ci et son client, puisque les doctrines américaines et françaises partagent une notion de confidentialité très large des communications entre l'avocat et le client. Toute violation de ce principe est généralement soumise à un encadrement **de nature judiciaire et non de nature administrative** le plus strict possible. *CEDH, 24 avril 1990, Huvig et Kruslin c/ France.*

La jurisprudence du Conseil constitutionnel reflète également ce souci de protection d'une des plus importantes libertés individuelles. Le Conseil Constitutionnel a d'ailleurs développé un véritable droit constitutionnel « de l'avocat », car le « recours et l'assistance d'un avocat constituent un droit constitutionnellement surveillé et garanti par le Conseil constitutionnel. » (Rentrée du Barreau de Paris Théâtre du Chatelet – 4 décembre 2009 Discours de M. Jean-Louis Debré, Président du Conseil constitutionnel « Le Conseil constitutionnel et les droits de la défense », disponible sur http://www.conseil-constitutionnel.fr/conseil-constitutionnel/root/bank_mm/discours_interventions/2009/jld_rentree_barreau_041209.pdf) (*CC, 19 et 20 janvier 1981, n° 80-127 DC, Loi renforçant la sécurité et protégeant la liberté des personnes, cons. 48 à 53,* censurant une disposition qui permettait au président d'une juridiction d'écarter de la salle d'audience un avocat dans des conditions portant atteinte aux droits de la défense ; *CC, 11 août 1993, n° 93-326 DC, Loi modifiant la loi n° 93-2 du 4 janvier 1993 portant réforme du code de procédure pénale, cons. 12* ; *CC, 2 janvier 1994, n°* 93-334 DC, *Loi instituant une peine incompressible et relative au nouveau code pénal et à certaines dispositions de procédure pénale, cons. 18* ; *CC, 2 mars 2004, n° 2004-492 DC, Loi portant adaptation de la justice aux évolutions de la criminalité, cons. 31,* reconnaissant le principe du libre entretien avec un avocat d'une personne gardée à vue qui constitue « un droit de la défense qui s'exerce durant la phase d'enquête de la procédure pénale » ; *CC, 30 juillet 2010, n° 2010-14/22 QPC, M. Daniel W. et autres (Garde à vue*), imposant l'assistance effective d'un avocat pour toute personne interrogée en garde à vue).

Or, l'accroissement de la mondialisation a donné lieu à l'internationalisation du droit et des contentieux. C'est ainsi que la représentation de clients localisés en France par des avocats résidents hors de France devient de plus en plus répandue. Il est ainsi de plus en plus courant pour ces avocats de communiquer habituellement par téléphone et par courriel avec leurs

clients basés en France et parfois avec les conseils français basés en France de ces clients dans le cadre de dossiers multi-juridictionnels.

D'après les statistiques du ministère de la Justice, au 1er janvier 2012, 2.506 avocats sont inscrits à la fois à un barreau français et à un barreau étranger, soit 4,5% des avocats. Sur les 1.384 avocats inscrits également dans un barreau d'un pays de l'Union européenne, près de la moitié le sont au Royaume-Uni (48%) et un quart se partagent entre l'Allemagne (14,2%) et la Belgique (11,3%). Hors Union européenne, près des deux-tiers sont inscrits dans un barreau des Etats-Unis (734) (Voir Statistiques sur la Profession d'Avocat, Situation au 1er Janvier 2012, disponible sur http://www.justice.gouv.fr/art_pix/1_1_commentaires2012.pdf). Ces statistiques restent muettes sur la localisation géographique des avocats admis à plusieurs barreaux.

Même si il n'y a pas de corrélation exacte entre le nombre d'avocats inscrits à la fois à un barreau français et dans un barreau étranger et leur présence physique en France ou à l'étranger, il est raisonnable d'estimer que le nombre d'avocats enregistrés dans un barreau français et pratiquant à l'étranger et, ce, hors du territoire national, s'élève à plusieurs milliers.

Par conséquent, la mise en cause de l'obligation de la règle de confidentialité pour les avocats localisés hors du territoire national ne constitue pas un problème marginal ou secondaire, mais constitue bien une question fondamentale.

La mise en place des techniques de recueil de renseignement et leur application au requérant, entre le 1er avril 2008 et le 27 juillet 2015, est de nature à annihiler le sacrosaint « secret professionnel » au-delà de l'encadrement judicaire pourtant déjà existant, et affecte l'intégrité de l' « attorney-client privilege » américain et du secret professionnel imposé par les barreaux français. Aux Etats-Unis, non seulement les juges rejettent l'ensemble des écoutes illicitement acquises, mais aussi toutes les preuves et éléments à charge qui pourraient en résulter, du fait de l'application stricte du 4e amendement de la Constitution Américaine. Voir *United States v. Renzi, et al.*, No. CR 08-00212, 2010 U.S. Dist. LEXIS 56092 (D. Ariz. June 2, 2010). Cette application stricte pourrait alors menacer la position de nos confrères par rapport à leurs clients dans le respect de leurs obligations de respect du secret professionnel, notamment vis-à-vis des barreaux américains concernés.

Cette violation systématique du caractère confidentiel des communications entre l'avocat localisé hors du territoire national et son client basé en France, entre le 1er avril 2008 et le 27 juillet 2015, et déclarée contraire à la Constitution par le Conseil Constitutionnel dans sa décision n° 2015-713 DC, menace donc la défense des intérêts des clients du requérant devant les juridictions américaines.

b. Le décret secret d'avril 2008 n'est opposable, ni aux requérants, ni à la CNIL, et, du fait de son illicéité, déclenchée par la décision n° 2015-713 DC du 26 juillet 2015 par le Conseil Constitutionnel, ne présente aucun obstacle à ce que la CNIL entreprenne des investigations et prononce les sanctions appropriées.

Le décret secret d'avril 2008 mentionné par les articles de presse indiqués ci-dessus, ne peut être opposé, soit aux requérants, soit à la CNIL, et ne peut permettre à la CNIL de décliner d'appliquer ses pouvoirs d'investigation et de sanction.

En effet, les lois et les actes administratifs existent dès leur promulgation ou leur signature mais leur entrée en vigueur est subordonnée à des mesures de publicité. Tant que la publication n'est pas intervenue, la norme nouvelle ne peut pas être opposée aux tiers (*CE, 13 décembre 1957, Barrot et autres, Rec. p. 675*) et elle ne peut ni être invoquée par eux, ni faire naître de droits à leur profit. Une loi ou un règlement qui n'a pas été publié ne peut servir de base légale à d'autres actes (*CE, 26 octobre 1956, Pubreuil, Rec. p. 389*).

Le Conseil d'État considère que si la promulgation rend un décret exécutoire, seule sa publication la rend opposable (*CE, 24 juin 2002, Ministre de la Défense c. Wolny, Req. n° 227983, Rec., tables, p. 605*, concluant à un défaut de publication au Journal officiel du décret du 27 novembre 1967 portant statut spécial des fonctionnaires titulaires de la direction générale de la sécurité extérieure. Nullité subséquente des actes négatifs intervenus sur son fondement).

De plus, le décret secret d'avril 2008 n'a fait l'objet d'aucune entrée en vigueur différée, ce qui constitue l'une des exceptions à ce principe de non-opposabilité. En tout état de cause, le différé de prise d'effet d'un acte règlementaire pris en application d'une loi serait soumis à un contrôle d'erreur manifeste d'appréciation par le juge administratif. Par exemple, en reportant en effet à une date trop lointaine l'entrée en vigueur d'une loi par le truchement d'une entrée en vigueur différée du règlement pris pour son application, l'autorité administrative méconnaît la volonté du législateur (*CE, 9 juillet 1993, Association « Collectif pour la défense du droit et des libertés », n° 139445*).

Enfin, concernant l'applicabilité du décret secret d'avril 2008, les défendeurs ne pourront s'abriter derrière la doctrine d'une disposition transitoire, qui permet, avant la publication de nouvelles normes, le maintien de certaines situations juridiques, ou de fixer des règles définissant un régime temporaire destiné à faciliter la transition vers un ordre législatif nouveau. En effet, le décret secret d'avril 2008 était basé sur la loi n° 91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des communications électroniques, et n'était donc pas une mesure de mise en place de la nouvelle loi sur le renseignement, adoptée plus de 8 ans après !

En dernier lieu, quelle que soit la valeur juridique intrinsèque qu'aurait pu détenir le décret secret d'avril 2008, celle-ci a été réduite à néant par la décision du Conseil Constitutionnel n° 2015-713 DC du 26 juillet 2015. En effet, cette décision déclare inconstitutionnelles les dispositions organisant la surveillance des communications émises ou reçues à l'étranger, surveillance qui était autorisée au nom des "intérêts fondamentaux de la Nation," car le législateur n'avait pas défini les conditions d'exploitation, de conservation et de destruction des données ainsi collectées, tout en se bornant à renvoyer ces questions à un décret en Conseil d'Etat. (Voir aussi *CC, 13 mars 2003, n° 2003-467 DC*, affirmant

> *« qu'il appartient au législateur, en vertu de l'article 34 de la Constitution, de fixer les règles concernant les garanties fondamentales accordées aux citoyens pour l'exercice des libertés publiques ; qu'il lui appartient notamment d'assurer la conciliation entre, d'une part, la sauvegarde de l'ordre public et la recherche des auteurs d'infractions, toutes deux nécessaires à la protection de principes et de droits de valeur constitutionnelle et, d'autre part, le respect de la vie privée et des autres droits et libertés constitutionnellement protégés. »)*

Le projet de loi concernant la surveillance internationale devant le parlement ne saurait être utilisé comme moyen d'appliquer une quelconque sauvegarde par la doctrine de rétroactivité quelconque aux fins d'excuser la CNIL d'exercer sa juridiction. En effet, le principe de non-rétroactivité des actes administratifs fait obstacle à ce qu'une règle nouvelle s'applique, au sens où elle les remettrait en cause, à des situations déjà constituées sous l'empire des anciennes règles (*CE, Ass., 25 juin 1948, Société du journal* L'Aurore, *n° 94511*).

La jurisprudence limitée autorisant une rétroactivité sous le contrôle du juge constitutionnel ne pourrait s'appliquer dans le cas présent, car, au regard des stipulations de l'article 6 § 1 de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, que l'intervention rétroactive du législateur au profit de l'État doit reposer sur d'impérieux motifs d'intérêt général et, au regard des stipulations de l'article 1er du premier protocole additionnel à cette convention, qu'un juste équilibre doit être ménagé entre l'atteinte aux droits découlant de lois en vigueur et les motifs d'intérêt général susceptible de la justifier (*CE, Ass., 27 mai 2005, Provin, n° 277975*). Ici, l'atteinte au secret professionnel des requérants ne pourrait permettre au juge constitutionnel ou administratif de trouver un tel équilibre.

De plus, la non-rétroactivité de la loi a valeur constitutionnelle en matière de répression pénale, entendue au sens large, incluant les sanctions administratives (*CC, 30 décembre 1982, n° 82-155 DC*). Etant donné les nombreuses conséquences pénales des actions des défendeurs, et des nombreuses dispositions pénales qui s'y appliquent (voir ci-dessous), le principe de non-rétroactivité s'applique pleinement, et l'absence de base juridique du décret secret d'avril 2008 permet donc à la CNIL d'appliquer pleinement ses pouvoirs d'investigations.

4. **La remise en cause par les défendeurs, du fait des techniques de surveillance incriminées entre le 1er avril 2008 et le 27 juillet 2015, entrainant la collecte et le traitement des données personnelles, du secret professionnel protégeant la profession d'avocat et l'obligation de confidentialité des échanges entre l'avocat et son client dans un contexte international entraine la qualification de ces actes par la CNIL de**

violations, infractions et de délits au sens de la Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés

a. Concernant le pouvoir d'injonction de la CNIL

Les articles 45 à 49 de la Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés définissent les conditions dans lesquelles la CNIL peut, soit enjoindre la cessation d'un traitement de données personnelles illicite (voir article 45 Alinéa II).

De plus, l'article 45 Aliéna III prévoit que :

> *[e]n cas d'atteinte grave et immédiate aux droits et libertés mentionnés à l'article 1er, le président de la commission peut demander, par la voie du référé, à la juridiction compétente d'ordonner, le cas échéant sous astreinte, toute mesure de sécurité nécessaire à la sauvegarde de ces droits et libertés.*

Or, dans le cas présent, les défendeurs se sont livrés à une obtention non autorisée ainsi qu'à une collecte et un traitement de données personnelles illicites sujettes à la juridiction et au contrôle de la CNIL.

En effet, les actions des défendeurs violent directement les termes des articles 6 et 7 de la Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. Les actions des défendeurs correspondent à la mise en œuvre de systèmes de collecte traitement de données à caractère personnel où les données n'ont pas été « *collectées et traitées de manière loyale et licite* ». Article 6 Aliéna 1. De plus, elles n'ont pas été « *collectées pour des finalités déterminées, explicites et légitimes* », puisque leur collecte depuis avril 2008 a été déclarée contraire à la constitution par la Conseil Constitutionnel. Article 6 Aliéna 2. Enfin, elles n'ont certainement pas été caractérisées comme « *adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et de leurs traitements ultérieurs* » du même fait de la décision n° 2015-713 DC du 26 juillet 2015 par le Conseil Constitutionnel. Article 6 Aliéna 3. Enfin, les actions des défendeurs n'ont très certainement pas reçu le consentement de la personne ou des requérants concernés. Ces actions n'ont pas non plus satisfait « *à une obligation légale incombant au responsable du traitement* » puisque le Conseil Constitutionnel, dans sa décision n° 2015-713 DC du 26 juillet 2015, a déclaré cette activité illicite dans la période avril 2008 à juillet 2015. Ces actions ne correspondent pas non plus à la « *réalisation de l'intérêt légitime poursuivi par le responsable du traitement ou par le destinataire, sous réserve de ne pas méconnaître l'intérêt ou les droits et libertés fondamentaux de la personne concernée.* » Article 7 alinéa 5.

De plus, dans un courrier daté du 15 septembre 2015, les requérants, aux motifs que le secret professionnel protégeant la profession d'avocat et l'obligation de confidentialité des

échanges entre l'avocat et son client dans un contexte international ont été directement affectées par le défendeur du fait de l'utilisation d'une interception des correspondances émises par voie de communications électroniques par une autorité publique, les requérants ont demandé à la Commission nationale de contrôle des interceptions de sécurité (« CNCIS ») (voir PJ n°4) :

- De procéder au contrôle de l'ensemble de ces interceptions de sécurité entre le 1er avril 2008 et le 25 juillet 2015 ;
- De déclarer que ces interceptions, en tant qu'elles ont été appliquées aux requérants, ont été effectuées en violation des dispositions de la loi n°91-646 du 10 juillet 1991 ;
- De déclarer que ces interceptions de sécurité, en tant qu'elles ont été appliquées aux requérants, représentent une violation de l'atteinte à la vie privée des requérants, et ce en violation de l'article 226-1 du Code Pénal ;
- De déclarer que ces interceptions de sécurité, en tant qu'elles ont été appliquées aux requérants, représentent une violation de l'atteinte au secret professionnel, et ce en violation de l'article 226-13 du Code Pénal ;
- De déclarer que ces interceptions de sécurité, en tant qu'elles ont été appliquées aux requérants, représentent une violation de l'atteinte au secret des correspondances, et ce en violation de l'article 226-15 du Code Pénal ;
- De recommander au Premier Ministre l'interruption immédiate de ces interceptions de sécurité ;
- De recommander au Premier Ministre la destruction immédiate de toutes les données accumulées au titre de ces interceptions de sécurité, et ce depuis la date du 1er avril 2008.

Du fait des violations de ces dispositions qui représentent également une atteinte grave, immédiate et continue depuis au moins avril 2008 aux droits et libertés des requérants, la CNIL a le pouvoir :

> [d']*exiger par injonction une cessation immédiate de [*ces obtentions et de ces traitements qui constituent du fait des violations du secret professionnel *...]*
> Article 45. Alinéa I. 2.
> [d']*engager une procédure d'urgence, définie par décret en Conseil d'État, pour […] décider l'interruption de la mise en œuvre du traitement,*
> Article 45. Alinéa II. 1.
>
> [de]*demander, par la voie du référé, à la juridiction compétente d'ordonner, le cas échéant sous astreinte, toute mesure de sécurité nécessaire à la sauvegarde de ces droits et libertés. En cas d'atteinte grave et immédiate aux droits et libertés mentionnés à l'article 1er, le président de la commission peut*

> *demander, par la voie du référé, à la juridiction compétente d'ordonner, le cas échéant sous astreinte, toute mesure de sécurité nécessaire à la sauvegarde de ces droits et libertés.*
> Article 45. Aliéna III.

L'une ou tous les moyens mentionnés ci-dessus sont applicables au cas présent.

b. Concernant les violations du chapitre IV de la Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés

Le chapitre IV de la Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés spécifie les formalités préalables à la mise en œuvre des traitements de données personnelles. Les articles 23 et 24 spécifient les conditions de déclaration et d'autorisation des traitements de données personnelles. L'article 26 prévoit une procédure particulière lorsque ces traitements sont mis en œuvre pour le compte de l'Etat :

> ***I.*** *- Sont autorisés par arrêté du ou des ministres compétents, pris après avis motivé et publié de la Commission nationale de l'informatique et des libertés, les traitements de données à caractère personnel mis en œuvre pour le compte de l'État et :*
> ***1°*** *Qui intéressent la sûreté de l'État, la défense ou la sécurité publique ;*
>
> ***2°*** *Ou qui ont pour objet la prévention, la recherche, la constatation ou la poursuite des infractions pénales ou l'exécution des condamnations pénales ou des mesures de sûreté.*
> *L'avis de la commission est publié avec l'arrêté autorisant le traitement.*
>
> ***II.*** *- Ceux de ces traitements qui portent sur des données mentionnées au I de l'article 8 sont autorisés par décret en Conseil d'État pris après avis motivé et publié de la commission ; cet avis est publié avec le décret autorisant le traitement.*

Or, aucune des mesures prises par la DGSE depuis avril 2008 et décrites ci-dessus n'ont fait l'objet d'aucune des procédures décrites à l'article 26, sans aucune exception.

c. Concernant certaines dispositions pénales de la Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés

i. Article 226-16 du Code Pénal

L'article 226-16 du Code Pénal prévoit que :

> *Le fait, y compris par négligence, de procéder ou de faire procéder à des traitements de données à caractère personnel sans qu'aient été respectées les formalités préalables à leur mise en œuvre prévues par la loi est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende.*

Or, tel qu'il est démontré au paragraphe précèdent, aucune formalité préalable à la mise en place de la collecte et du traitement de données personnelles identifiées ci-dessus n'a été effectuée par les défendeurs. Par conséquent, cet article s'applique pleinement, et les requérants demandent par conséquent que la CNIL, en application de l'article 11-2°-e) de la Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, informe « *sans délai le procureur de la République, conformément à l'article 40 du code de procédure pénale, des infractions dont elle a connaissance*. »

ii. Article 226-18 du Code Pénal

L'article 226-18 du Code Pénal prévoit 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.*

Or, tel qu'il est démontré au paragraphe précèdent, la collecte et le traitement des données à caractère personnel par les défendeurs a été déclarée illicite par la décision du Conseil Constitutionnel n° 2015-713 DC en date du 26 juillet 2015. Par conséquent, cet article s'applique pleinement, et les requérants demandent par conséquent que la CNIL, en application de l'article 11-2°-e) de la Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, informe « *sans délai le procureur de la République, conformément à l'article 40 du code de procédure pénale, des infractions dont elle a connaissance*. »

iii. Article 226-20 du Code Pénal

L'article 226-20 du Code Pénal prévoit que :

> *Le fait de conserver des données à caractère personnel au-delà de la durée prévue par la loi ou le*

> *règlement, par la demande d'autorisation ou d'avis, ou par la déclaration préalable adressée à la Commission nationale de l'informatique et des libertés, est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende, sauf si cette conservation est effectuée à des fins historiques, statistiques ou scientifiques dans les conditions prévues par la loi.*
> *Est puni des mêmes peines le fait, hors les cas prévus par la loi, de traiter à des fins autres qu'historiques, statistiques ou scientifiques des données à caractère personnel conservées au-delà de la durée mentionnée au premier alinéa.*

Or, tel qu'il est démontré au paragraphe précèdent, comme aucune formalité préalable à la mise en place de systèmes de collecte et de traitement des données à caractère personnel identifiées ci-dessus n'a été effectuée par les défendeurs, ceux-ci, qui ont maintenu à la fois les données et leur procédures de traitement durant une période de 8 ans, ont maintenu ces données par devers eux au-delà de toute période propret autorisée par la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. Par conséquent, cet article s'applique pleinement, et les requérants demandent par conséquent que la CNIL, en application de l'article 11-2°-e) de la Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, informe « *sans délai le procureur de la République, conformément à l'article 40 du code de procédure pénale, des infractions dont elle a connaissance*. »

iv. Article 226-21 du Code Pénal

L'article 226-21 du Code Pénal prévoit que :

> *Le fait, par toute personne détentrice de données à caractère personnel à l'occasion de leur enregistrement, de leur classement, de leur transmission ou de toute autre forme de traitement, de détourner ces informations de leur finalité telle que définie par la disposition législative, l'acte réglementaire ou la décision de la Commission nationale de l'informatique et des libertés autorisant le traitement automatisé, ou par les déclarations préalables à la mise en œuvre de ce traitement, est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende.*

Or, tel qu'il est démontré au paragraphe précèdent, la collecte et le traitement des données à caractère personnel par les défendeurs, ayant été déclarée illicite par la décision du Conseil Constitutionnel n° 2015-713 DC en date du 26 juillet 2015, a rendu cette collecte également contraire aux finalités définies par la loi de la Loi n°91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des communications électroniques. En effet, tel que l'ont demandé les requérants à la Commission nationale de contrôle des interceptions de sécurité, les actions de défendeurs, aux motifs que le secret professionnel protégeant la profession d'avocat et l'obligation de confidentialité des échanges entre l'avocat et son client dans un contexte international ont été directement affectées par le défendeur du fait de l'utilisation d'une interception des correspondances émises par voie de communications électroniques par une autorité publique.

Par conséquent, les actions des défendeurs ont permis à ceux-ci de « *détourner ces informations de leur finalité telle que définie par la disposition législative*, » finalité définie par la loi de la Loi n°91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des communications électroniques. Par conséquent, cet article s'applique pleinement et les requérants demandent par conséquent que la CNIL, en application de l 'article 11 2° e) de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, informe « *sans délai le procureur de la République, conformément à l'article 40 du code de procédure pénale, des infractions dont elle a connaissance.* »

v. Article 226-22 du Code Pénal

L'article 226-22 du Code Pénal prévoit que :

> *Le fait, par toute personne qui a recueilli, à l'occasion de leur enregistrement, de leur classement, de leur transmission ou d'une autre forme de traitement, des données à caractère personnel dont la divulgation aurait pour effet de porter atteinte à la considération de l'intéressé ou à l'intimité de sa vie privée, de porter, sans autorisation de l'intéressé, ces données à la connaissance d'un tiers qui n'a pas qualité pour les recevoir est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende.*

Or, tel qu'il est démontré au paragraphe précédent, les défendeurs Alcatel-Luce et Orange ont contribué, en assistant à la mise en place des systèmes de collecte et de de traitement de données personnelles et en permettant à la DGSE les accès aux câbles sous-marins (voir paragraphe 1.a et 1.c de la présente requête), ont

> *recueilli, à l'occasion de leur enregistrement, de leur*

> *classement, de leur transmission ou d'une autre forme de traitement, des données à caractère personnel dont la divulgation aurait pour effet de porter atteinte à la considération de l'intéressé ou à l'intimité de sa vie privée, de porter, sans autorisation de l'intéressé, ces données à la connaissance d'un tiers qui n'a pas qualité pour les recevoir*

Par conséquent, cet article s'applique pleinement et les requérants demandent par conséquent que la CNIL, en application de l 'article 11 2° e) de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, informe « *sans délai le procureur de la République, conformément à l'article 40 du code de procédure pénale, des infractions dont elle a connaissance.* »

vi. Article 226-24 du Code Pénal

L'article 226-24 du Code Pénal prévoit que :

> *Les personnes morales peuvent être déclarées responsables pénalement, dans les conditions prévues par l'article 121-2, des infractions définies à la présente section.*
> *Les peines encourues par les personnes morales sont :*
> *1° L'amende, suivant les modalités prévues par l'article 131-38 ;*
> *2° Les peines mentionnées aux 2°, 3°, 4°, 5°, 7°, 8° et 9° de l'article 131-39.*
> *L'interdiction mentionnée au 2° de l'article 131-39 porte sur l'activité dans l'exercice ou à l'occasion de l'exercice de laquelle l'infraction a été commise.*

Or, tel qu'il est démontré au paragraphe précèdent, les actes incrimines, sujets soit à des procédures de sanctions soit à des articles du code pénal, ont bien été commises par des personnes morales, Alcatel-Lucent et Orange, ainsi que par la DGSE, personne moral autonome dépositaires de l'autorité publique.

d. <u>Les défendeurs ne peuvent opposer les conditions de l'Article 226-10 du Code Pénal à la présente requête.</u>

Aux termes de l'Article 226-10 du Code Pénal, une personne physique ou morale incriminée par une plainte au pénal peut citer son auteur pour dénonciation calomnieuse si

> *« [l]a dénonciation, effectuée par tout moyen et dirigée contre une personne déterminée, d'un fait qui est de nature à entraîner des sanctions judiciaires, administratives ou disciplinaires et que l'on sait totalement ou partiellement inexact, lorsqu'elle est adressée soit à un officier de justice ou de police administrative ou judiciaire, soit à une autorité ayant le pouvoir d'y donner suite ou de saisir l'autorité compétente, soit aux supérieurs hiérarchiques ou à l'employeur de la personne dénoncée, est punie de cinq ans d'emprisonnement et de 45 000 euros d'amende. La fausseté du fait dénoncé résulte nécessairement de la décision, devenue définitive, d'acquittement, de relaxe ou de non-lieu, déclarant que le fait n'a pas été commis ou que celui-ci n'est pas imputable à la personne dénoncée.*

Pour que la plainte en dénonciation calomnieuse aboutisse, il faut que les défendeurs démontrent que, pour prouver l'intention frauduleuse du requérant, celui-ci était de mauvaise foi au moment du dépôt de la plainte. Les défendeurs devront donc montrer que le requérant, non seulement a menti dans ses déclarations, mais savait qu'il mentait en les soumettant à la CNIL. Cette démonstration ne peut être effectuée sans que, soit le requérant ait imputé des faits aux défendeurs qu'il savait faux, soit que le requérant a embelli les faits, les a dénaturés ou présentés sous des apparitions mensongères, à tel point que la plainte devienne choquante et délictuelle. Le fait de soumettre des faits vrais mais à qui le requérant donne une fausse qualification ne constitue pas un délit de dénonciation calomnieuse.

Dans le cas présent, tous les faits soumis à votre attention sont vrais, vérifiés, et accompagnés de sources gouvernementales ou journalistiques vérifiables et crédibles. De plus, tous les faits soumis à votre attention correspondent aux éléments des délits mentionnés dans les articles cités du Code Pénal. Par conséquent, la qualification pénale des faits reprochés est fondée sur une analyse objective et raisonnable des articles du Code Pénal retenus. Les requérants seront donc dans l'impossibilité de prouver l'intention frauduleuse du requérant, sa mauvaise foi, ou un quelconque mensonge. De plus, aucun des faits soumis à votre attention ont été dénaturés ou présentés sous des apparitions mensongères, puisque ces sources indiquées sont toutes des sources vérifiables et crédibles, et que ces faits ont été analysés sans autre contexte que les conditions des qualifications requises par chaque article du Code Pénal retenu.

Par conséquent, les défendeurs seront dans l'impossibilité de soutenir une plainte en dénonciation calomnieuse du fait de la plainte soumise devant vous.

5. La demande des requérants

Aux motifs que,

- la remise en cause par les défendeurs, du fait des techniques de surveillance incriminées entre le 1er avril 2008 et le 26 juillet 2015, du secret professionnel protégeant la profession d'avocat et l'obligation de confidentialité des échanges entre l'avocat et son client dans un contexte international représente un grave préjudice que la CNIL se doit d'identifier, pour lequel elle doit formuler un avis et entreprendre les investigations nécessaires ;
- les défendeurs se sont livrés à une obtention non autorisée ainsi qu'à un traitement de données personnelles illicites sujettes à la juridiction et au contrôle de la CNIL ;

Les requérants demandent à la CNIL :

- De procéder au contrôle de l'ensemble de ces collectes et traitements de données personnelles ayant eu lieu entre le 1er avril 2008 et le 26 juillet 2015 ;
- De déclarer que ces collectes et traitements de données personnelles, en tant qu'elles ont été appliquées aux requérants, ont été effectuées en violation des dispositions de des articles 6 et 7 de la Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ;
- De déclarer que ces collectes et traitements de données personnelles, en tant qu'elles ont été appliquées aux requérants, ont été effectuées en violation des dispositions de des articles 23 et 24 de la Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ;
- De déclarer que ces collectes et traitements de données personnelles, en tant qu'elles ont été appliquées aux requérants, représentent une violation des articles 226-16, 226-18, 226-20, 226-21, 226-22, 226-24 du Code Pénal ;
- De demander au Premier Ministre l'interruption immédiate de ces collectes et traitements de données personnelles ;
- De demander au Premier Ministre la destruction immédiate de toutes les données accumulées au titre de ces collectes et traitements de données personnelles et ce depuis la date du 1er avril 2008.

En vous remerciant par avance de votre réponse, je vous prie, Monsieur le Président, de bien vouloir agréer l'assurance de nos sentiments distingués.

Pierre Ciric, Esq.
Member of the Firm

cc: Jean-Marie Delarue
Conseiller d'État honoraire
Président
Commission nationale de contrôle des interceptions de sécurité (« CNCIS »)
35, rue Saint-Dominique
75700 Paris SP 07
Téléphone : +33 1 45 55 70 20
Télécopie : +33 1 45 51 08 71
Par Courriel : president.cncis@pm.gouv.fr

Olivier Guérin
Délégué général
Commission nationale de contrôle des interceptions de sécurité
35, rue Saint-Dominique
75700 Paris SP 07
Téléphone :+33 1 45 55 70 20
Télécopie :+33 1 45 51 08 71
Par Courriel : deleguegeneral.cncis@pm.gouv.fr, olivier.guerin@pm.gouv.fr

Mme Patricia Adam
Commission de la défense nationale et des forces armées
Assemblée Nationale
126 rue de l'Université
75355 PARIS 07 SP
FRANCE
Ph: +33 1 40 63 60 00
Par courriel : padam@assemblee-nationale.fr

Thomas Vandenabeele
Président
French American Bar Association, Inc.
34-35 76th st., # 1-O,
Jackson Heights, NY 11372
Par courriel: tv@khgflaw.com

À l'attention des Sénatrices et Sénateur

À l'attention des Députées et Députés

À l'attention des Conseillères et Conseillers Consulaires, élues et élus à l'assemblée des Français de l'Etranger aux Etats-Unis