SPINOSI & SUREAU
SCP d'Avocat au Conseil d'Etat
et à la Cour de cassation
16 Boulevard Raspail
75007 PARIS

CONSEIL D'ÉTAT

SECTION DU CONTENTIEUX

OBSERVATIONS COMPLEMENTAIRES

POUR **:** **1/ La Quadrature du Net**

2/ French Data Network

3/ La Fédération des fournisseurs d'accès à Internet associatifs

SCP SPINOSI & SUREAU

CONTRE **:** 1/ Le Premier ministre

2/ Ministre de l'intérieur

2/ Ministre des armées

Sur la requête n° 394.922

I. Persistant dans l'ensemble des moyens et conclusions développés dans ses précédentes écritures, les associations exposantes entendent présenter les observations complémentaires suivantes, notamment aux fins de répliquer aux observations ministérielles et soulever les moyens complémentaires suivants.

II. A titre liminaire, les associations rappellent qu'à la suite de la question prioritaire de constitutionnalité qu'elles ont posé à l'encontre des dispositions de l'article L. 811-51 du code de la sécurité intérieure, le Conseil constitutionnel a censuré ces dispositions aux motifs qu'elles portent « *une atteinte manifestement disproportionnée au droit au respect de la vie privée et au secret des correspondances* » (Conseil constit., Déc. n° 2016-590 QPC du 21 octobre 2016).

Sur l'applicabilité de la Charte des droits fondamentaux de l'Union européenne

III. En premier lieu, dans ses observations en défense, le ministre de l'intérieur soutient que les mesures attaquées par les associations requérantes n'entrent pas dans le champ d'application du droit de l'Union, de sorte que la Charte des droits fondamentaux de l'Union européenne ainsi que les autres instruments de droit dérivés – en particulier la directive 2002/58/CE du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques et la directive 2000/31/CE du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur – ne seraient pas invocables dans le présent litige.

Au surplus, le ministre avance que, à supposer même que l'accès des services de renseignement aux données de connexion relève des mesures prévues à l'article 15, paragraphe 1, de la directive 2002/58/CE, l'invocation de la Charte demeurerait inopérante.

Or, rien n'est moins vrai.

III-1 En effet, force est de constater que ces affirmations, portées par le ministre dans ses écritures du 4 juillet 2016, ont été directement et indiscutablement contredites par la Cour de justice de l'Union européenne, dans l'arrêt *Tele 2*, tant sur le champ d'application du droit de l'UE et de la Charte, que sur l'interprétation de l'article 15 de la directive 2002/58 (CJUE, g^{de} ch., 21 déc. 2016, *Tele2 Sverige*, C-203/15, C-698/15).

Ainsi, la Cour de justice a très clairement énoncé que :

« *Eu égard à l'économie générale de la directive 2002/58, les éléments relevés au point précédent du présent arrêt n'autorisent pas à conclure que les mesures législatives visées à l'article 15, paragraphe 1, de la directive 2002/58 seraient exclues du champ d'application de cette directive, sauf à priver cette disposition de tout effet utile.*

En effet, ladite disposition présuppose nécessairement que les mesures nationales qui y sont visées, telles que celles relatives à la conservation de données à des fins de lutte contre la criminalité, relèvent du champ d'application de cette même directive, puisque cette dernière n'autorise expressément les États membres à les adopter que dans le respect des conditions qu'elle prévoit » (CJUE, g^{de} ch., 21 déc. 2016, *Tele2 Sverige*, C-203/15, C-698/15, point 73).

Ainsi, les mesures entravant l'article 5 de la directive 2002/58 pour les motifs énoncés à l'article 15, paragraphe 1, de la même directive tombent nécessairement dans le champ d'application du droit de l'Union.

Plus précisément, la grande chambre de la Cour de justice a décidé que :

« *En effet, la protection de la confidentialité des communications électroniques et des données relatives au trafic y afférentes, garantie à l'article 5, paragraphe 1, de la directive 2002/58, s'applique aux mesures prises par* ***toutes les personnes*** *autres que les utilisateurs, qu'il s'agisse de personnes ou d'entités privées ou d'entités étatiques. Comme le confirme le considérant 21 de cette directive, celle-ci vise à* ***empêcher « tout accès »*** *non autorisé aux communications,* ***y compris à « toute donnée afférente à ces communications », afin de protéger la confidentialité des communications électroniques*** (§ 77).

[…]

Le principe de confidentialité des communications instauré par la directive 2002/58 implique, entre autres, ainsi qu'il ressort de l'article 5, paragraphe 1, deuxième phrase, de celle-ci, une interdiction faite, en principe, à toute autre personne que les utilisateurs de stocker, sans le consentement de ceux-ci, les données relatives au trafic afférentes aux communications électroniques. Font seuls l'objet d'exceptions les personnes légalement autorisées conformément à l'article 15, paragraphe 1, de cette directive […] » (§ 85).

L'article 5 de la directive 2002/58 s'applique donc pleinement aux mesures des autorités nationales ayant pour objet l'accès aux données de connexion ainsi qu'aux mesures d'interception du contenu des réseaux de communications électroniques.

Dès lors, de telles mesures nationales relèvent du champ d'application du droit de l'Union et doivent, pour cette raison, être limitées au strict nécessaire conformément aux exigences de la Charte, lesquelles sont parfaitement opposables à ces mesures nationales.

III-2 Or, en l'occurrence, la plupart des techniques de recueil de renseignement instituées par la loi du 24 juillet 2015 et ses décrets d'application portent sur des accès aux communications électroniques transmises sur des réseaux de communications électroniques.

Cela vaut notamment pour toutes les mesures de surveillance internationale, de recueil de données de connexion, d'accès aux données de connexion en temps réel, de traitements algorithmiques sur des données de connexion ou encore d'interceptions de sécurité.

Dès lors, il ne fait aucun doute que les mesures en cause ont pour objet principal — si ce n'est exclusif — l'accès aux données des communications électroniques, qu'il s'agisse du contenu ou de métadonnées, notamment celles traitées et acheminées sur des réseaux de communications électroniques visés par la mise en œuvre de techniques de renseignement.

L'entrave que ces mesures constituent au regard du principe de confidentialité desdites communications est affirmée de manière constante et sans aucune ambiguïté par la Cour de justice.

III-3 Par conséquent, les techniques de recueil de renseignements en cause doivent être conformes au droit de l'Union et notamment aux directives 2000/31 et 2002/58 interprétées à la lumière de la Charte ainsi qu'aux articles 7, 8, 11 et 52, paragraphe 1, de la Charte elle-même.

À ce titre, les associations exposantes ne peuvent que renvoyer à leurs observations relatives à la disproportion des dispositions attaquées (cf. **observations complémentaires aux points IX et s.**).

En tout état de cause, les exposantes rappellent que si le Conseil d'État venait à s'interroger sur les modalités d'application du droit de l'Union en l'espèce, celui-ci serait alors tenu de transmettre à la Cour de justice les questions correspondantes telles que formulées par les parties requérantes (cf. **le dispositif des observations complémentaire**).

Sur la méconnaissance des exigences tirées des articles 8 et 13 de la Convention européenne des droits de l'homme concernant l'insuffisance des mécanismes compensant l'absence de notification *a posteriori*

IV. En deuxième lieu, le ministre soutient que l'absence de mécanisme de notification *a posteriori* en l'espèce ne saurait suffire à caractériser une violation des articles 8 et 13 de la Convention, dès lors que le dispositif attaqué serait assorti, à tous les stades de la procédure, de modalités de contrôle constituant des garanties suffisantes au sens de la Convention (Cour EDH, Plén., 6 sept. 1978, *Klass c. All.*, n° 5029/71 ; Cour EDH, g^de ch., 4 déc. 2015, *Zakharov c. Russie*, n° 47143/06).

À ce titre, le ministre considère que la jurisprudence européenne offre la possibilité de déroger à l'exigence de notification *a posteriori* lorsqu'elle risque de « *compromettre le but à long terme* » de la surveillance ou encore de « *contribuer à révéler les méthodes de travail* » et ainsi « *ne saurait en soi justifier la conclusion que l'ingérence n'était pas nécessaire dans une société démocratique, car*

c'est précisément cette absence d'information qui assure l'efficacité de la mesure constitutive de l'ingérence » (CEDH, g^de^ ch., 4 déc. 2015, *Zakharov c. Russie*, n^o^ 47143/06, §287).

Cette absence de notification serait compensée par l'instauration d'autres mesures permettant d'assurer un recours effectif aux personnes intéressées par la mesure de surveillance en l'espèce.

D'une part, le ministre fait valoir que la loi du 24 juillet 2015 relative au renseignement, en créant la Commission nationale de contrôle des techniques de renseignement (CNCTR), confie la supervision des mesures de surveillance « *à un organe de contrôle externe ayant le statut d'autorité administrative indépendante et disposant de garanties liées à ce statut* » (mémoire en défense produit dans l'affaire n^o^394925), p. 5).

Au titre desdites garanties, il allègue principalement celle tirée de l'article L. 832-1 du code de la sécurité intérieure prévoyant que « *dans l'exercice de leurs fonctions, les membres de la commission ne reçoivent d'instruction d'aucune autorité* ».

Les articles L. 833-2 et L. 833-3 du code de la sécurité intérieure compléteraient ce dispositif en précisant respectivement que la Commission nationale de contrôle des techniques de renseignement « *dispose d'un accès permanent, complet et direct aux relevés, registres, renseignements collectés, transcriptions et extractions mentionnés au [livre VIII du code de la sécurité intérieure] et […] est informée à tout moment, à sa demande, des modalités d'exécution des autorisations en cours* » et que « *le fait d'entraver l'action de la commission [est puni d'un an d'emprisonnement et de 15 000 € d'amende]* ».

D'autre part, le ministre affirme que la Commission dispose, en vertu de l'article L. 821-1 du code de la sécurité intérieure, de pouvoirs de contrôle préalable renforcés et peut, sur le fondement de l'article L. 833-4 du même code, de sa propre initiative ou à la suite d'une réclamation, vérifier que les mesures de surveillance ont été ou sont mises en œuvre conformément aux exigences légales. Dans ce cadre, elle notifie à l'auteur de la réclamation qu'elle a procédé aux vérifications attendues, sans en préciser le sens.

Au surplus, le ministre ajoute que la Commission nationale de contrôle des techniques de renseignement est dotée d'un pouvoir de recommandation lui permettant d'inviter le Premier ministre à cesser la mise en œuvre d'une technique de renseignement irrégulière.

En l'absence de suites ou si celles-ci sont jugées insuffisantes, la Commission nationale de contrôle des techniques de renseignement, ou au moins trois de ses membres, peuvent saisir le Conseil d'Etat qui, le cas échéant, pourra annuler l'autorisation accordée et enjoindre de procéder à la destruction des renseignements irrégulièrement collectés (article L. 833-8 du code de la sécurité intérieure et article L. 773-7 du code de justice administrative).

Le ministre distingue la situation en l'espèce des circonstances de faits et de droit relevés dans la jurisprudence de la Cour et notamment ses décisions *Zakharov* et *Szabo Vissy* précitées, en soulignant qu'il est possible, tout d'abord, de contester la mise en œuvre de techniques de renseignement de façon effective — le ministre invoque à l'appui de cet argument la trentaine de requêtes enregistrées au jour du dépôt de son mémoire en défense.

Selon le ministre ces éléments constituent des garanties suffisantes au regard des exigences énoncées par la Cour européenne.

Toutefois, une telle argumentation ne saurait convaincre.

IV-1 Tout d'abord, ainsi que les parties requérantes l'ont déjà amplement démontré dans leurs précédentes écritures, aucun mécanisme de droit interne ne permet de compenser, comme requis par la Cour européenne des droits de l'homme, l'inexistence de la procédure de notification (cf. **mémoire complémentaire aux points IX-1 et s.**).

Non seulement, les personnes concernées ne disposent strictement d'aucune information telle que requise par la Cour européenne des droits de l'homme.

Mais en outre, le mécanisme d'information prévu par les articles L. 833-4 et L. 841-1 du code de la sécurité intérieure ne saurait passer pour « *une possibilité satisfaisante de demander et d'obtenir auprès des*

autorités des informations sur les interceptions » (Cour EDH, g^{de} ch., 4 déc. 2015, *Zakharov c. Russie*, n^{o} 47143/06, § 298) au sens des exigences tirées des articles 8 et 13 de la Convention.

IV-2 Ensuite, il suffit de distinguer le cas des mesures portant sur des communications nationales de celles portant sur des communications internationales pour faire apparaître que la conventionalité du dispositif n'est aucunement assurée.

IV-2.1 S'agissant des mesures portant sur les communications nationales, les associations requérantes ont déjà démontré que la procédure instituée par les articles L. 773-1 et s. du code de la justice administrative ne respecte en rien le principe du contradictoire notamment en ce que l'administration, partie à la procédure, est maître de ce qui entre dans le champ du secret de la défense nationale et donc des éléments pouvant être partagés ou non avec la partie requérante.

Étant rappelé que, contrairement à d'autres États membres, aucun mécanisme de représentation par des avocats habilités au secret défense n'a été créé.

Ainsi, l'introduction du secret défense dans les procédures contentieuses, présentée par le ministre comme une avancée, ne constitue en réalité qu'un profond recul du procès équitable et ne saurait en tout état de cause compenser l'inexistence d'une notification des personnes concernées par les techniques de renseignement portant sur les communications nationales.

IV-2.2 De manière tout à fait déterminante, les personnes concernées ne disposent d'absolument aucun recours en matière de surveillance internationale, ni d'aucune notification sur les techniques de renseignement portant sur leurs communications internationales transitant par des réseaux de communications électroniques visés à l'article L. 854-2 du code de la sécurité intérieure.

IV-2.2.1 D'une part, l'article L. 854-1 du code de la sécurité intérieure dispose que la surveillance internationale « *est exclusivement régie par le présent chapitre* ».

La possibilité pour les justiciables de se tourner vers la Commission nationale de contrôle des techniques de renseignement et le Conseil d'État n'est donc pas garantie par la loi lorsque sont en cause des mesures de surveillance internationale.

Cela est confirmé par l'article L. 854-9 du code de la sécurité intérieure qui, dans le chapitre « surveillance internationale » du code de la sécurité intérieure, dispose que :

« *Sur réclamation de toute personne souhaitant vérifier qu'aucune mesure de surveillance n'est irrégulièrement mise en œuvre à son égard, la commission s'assure que les mesures mises en œuvre au titre du présent chapitre respectent les conditions qu'il fixe* ».

Cet article, qui reproduit l'article L. 833-4 précité, implique en effet que les articles L. 833-4 et L. 841-1 ne sont pas applicables au chapitre encadrant la surveillance internationale.

IV-2.2.2 D'autre part, l'article L. 773-1 du code de justice administrative (CJA) implique que le Conseil d'État ne peut être saisi que sur le fondement de l'article L. 841-1.

L'absence de recours devant le Conseil d'État est confirmée par la jurisprudence du Conseil constitutionnel, selon lequel « *la personne faisant l'objet d'une mesure de surveillance internationale ne peut saisir un juge pour contester la régularité de cette mesure* » (Conseil constit., 26 nov. 2015, *Loi surveillance internationale*, 2015-722 DC, cons. 18).

Par conséquent, il apparaît donc que deux catégories de personnes doivent être distinguées :

- Ceux utilisant des « numéros d'abonnement ou des identifiants techniques rattachables au territoire national » au sens de l'article L. 854-1 du code de la sécurité intérieure, lesquels bénéficient d'un droit au recours édulcoré et insuffisant au

regard des exigences de la Cour européenne des droits de l'homme ;

- Les autres, ne bénéficiant d'absolument aucun droit.

Pourtant, la Cour européenne des droits de l'homme ne fait pas de distinction selon la nature des numéros ou identifiants utilisés.

Il importe d'ailleurs de relever que la formulation empruntée à l'article L. 854-1 du code de la sécurité intérieure est pour le moins spécieuse. À l'heure où une immense partie des communications est entièrement numérique et transite entre de multiples prestataires (fournisseur de messagerie en ligne, opérateur grand public, transitaire, etc.), la notion d'« *identifiant technique rattachable au territoire national* » est pour le moins inconsistante.

La notion demeure indéfinie et la distinction entre les deux formes de communication, déjà injustifiée, est dénuée de toute pertinence en pratique dans de nombreux contextes, notamment celui des communications électroniques transitant par Internet.

En définitive, le Conseil d'Etat ne pourra manquer de faire droit aux prétentions des exposantes.

Sur la méconnaissance du droit à un recours effectif et du droit à un procès équitable

V. En troisième lieu, les associations exposantes entendent attirer l'attention du Conseil d'Etat sur un récent arrêt rendu par la Grande Chambre de la Cour européenne des droits de l'homme qui vient conforter un peu plus encore leur démonstration selon laquelle les dispositions du livre VIII du code de la sécurité intérieure intitulé « *Du renseignement* » ainsi que les dispositions des articles L. 773-1 à L. 773-8 du code de justice administrative, telles qu'issues de la loi n° 2015-912 du 24 juillet 2015 relative au renseignement, portent atteinte au droit à un recours effectif et au droit à un procès équitable, dont dérive tout particulièrement le principe du contradictoire.

V-1 En effet, et en droit, il importe de relever que la Cour européenne des droits de l'homme opère une mise en balance entre les droits des justiciables et les raisons soulevées par les Etats susceptibles de justifier la non-divulgation de certaines preuves pertinentes, telles que la sécurité nationale, afin de déterminer si le droit à un procès équitable n'a pas été méconnu.

A cet égard, et selon une jurisprudence désormais établie, si le droit à la divulgation des preuves n'est pas absolu, « *toutes difficultés causées à la défense par une telle limitation doivent être suffisamment compensées par la procédure suivie devant les autorités judiciaires* » (CEDH, g^{de} ch., *Fitt c. Royaume-Uni*, Req. n° 29777/96, § 45). La Cour examine ainsi que « *le processus décisionnel a satisfait dans toute la mesure du possible aux exigences du contradictoire et de l'égalité des armes et s'il était assorti de garanties aptes à protéger les intérêts de l'accusé* » (*Ibid.* §46).

Une illustration d'un tel examen a été récemment et solennellement donnée par la Cour dans son arrêt *Regner c. République Tchèque* (CEDH, g^{de} ch., 19 sept. 2017, Req. n°35289/11). Lorsque certains documents font l'objet d'une classification, de nouveaux critères sont fixés afin de rechercher « *si les limitations aux principes du contradictoire et de l'égalité des armes, tels qu'applicables dans la procédure civile, ont été suffisamment compensées par d'autres garanties procédurales* » (*Ibid.* §151), et ce, au regard du contrôle que possède l'autorité judiciaire sur les pièces classifiées.

Pour la Cour, la « *capacité des juges à apprécier les faits de l'espèce de manière adéquate* » n'a pu être remise en cause « *au motif qu'ils n'ont pas eu un accès intégral aux documents pertinents* » (*Ibid*. §152), car ceux-ci disposaient de garanties suffisantes, exhaustivement développées dans l'arrêt.

Ainsi, « *les tribunaux ont accès à tous les documents classifiés, sans restriction, sur lesquels l'Office s'est basé pour justifier sa décision. Ils ont ensuite le pouvoir de se livrer à un examen approfondi des raisons invoquées par l'Office pour ne pas communiquer les pièces classifiées. Ils peuvent en effet apprécier la justification de la non-communication des pièces classifiées et ordonner la communication de celles dont ils estimeraient qu'elles ne méritent leur classification* » (*Ibid*. §152).

La non-divulgation des preuves est donc compensée par la capacité des autorités judiciaires à examiner les motifs d'une mesure de renseignement, et à disposer d'un large pouvoir sur les pièces classées liées à cette mesure.

V-2 Or, en l'occurrence, il est manifeste que les dispositions des articles L. 773-1 à L. 773-8 du code de justice administrative, telles qu'issues de la loi n° 2015-912 du 24 juillet 2015 relative au renseignement, ne répondent pas à de telles garanties.

Plus précisément encore, il n'existe aucune compensation à la limitation au principe du contradictoire provoquée par le secret défense.

En effet, l'article L. 773-2 du code de justice administrative dispose notamment que « *dans le cadre de l'instruction de la requête, les membres de la formation de jugement et le rapporteur public sont autorisés à connaître de l'ensemble des pièces en possession de la Commission nationale de contrôle des techniques de renseignement* ». Il n'est ainsi aucunement précisé si les pièces ayant justifié la mise en œuvre de la mesure de renseignement font partie des pièces connues par la formation de jugement.

Ensuite, les dispositions législatives ne permettent aucunement au juge de procéder à un examen approfondi des raisons invoquées par les autorités pour mettre en place une mesure de renseignement. En vertu de l'article L. 773-6 du code de justice administrative, le juge possède uniquement la capacité de constater une absence d'illégalité « *sans confirmer ni infirmer la mise en œuvre d'une technique* ».

Dans le cas d'une mesure déclarée illégale, l'article L.773-7 du code de justice administrative permet seulement au juge « *d'annuler l'autorisation et ordonner la destruction des renseignements irrégulièrement collectés* » sans, à nouveau, la soumettre à un examen approfondi.

Par ailleurs, l'article L.773-7 du même code dispose en son deuxième alinéa que « *sans faire état d'aucun élément protégé par le secret de la défense nationale, elle informe la personne concernée ou la juridiction de renvoi qu'une illégalité a été commise.* »

Il n'existe donc strictement aucune possibilité pour le juge d'assortir à cette information, la communication d'une pièce justifiant la mesure déclarée illégale.

Enfin, le troisième alinéa de l'article L.773-7 dispose que « *Lorsque la formation de jugement estime que l'illégalité constatée est susceptible de constituer une infraction, elle en avise le procureur de la République et transmet l'ensemble des éléments du dossier au vu duquel elle a statué à la Commission consultative du secret de la défense nationale, afin que celle-ci donne au Premier ministre son avis sur la possibilité de déclassifier tout ou partie de ces éléments en vue de leur transmission au procureur de la République ».*

Or, les avis de la Commission du secret de la défense nationale ne sont pas impératifs.

Si le juge peut éventuellement demander à ce qu'une pièce soit déclassifiée – étant rappelé qu'il ne sera pas nécessairement fait droit à une telle demande –, il ne peut en aucun cas l'ordonner.

Par conséquent, les dispositions en cause ne sont pas conformes aux exigences posées par la Cour européenne des droits de l'homme permettant de garantir le droit à un procès équitable.

De ce chef aussi, l'annulation des dispositions du décret litigieux s'impose faute de base légale.

Sur la méconnaissance des engagements internationaux de la France par l'article 323-8 du code pénal, tel qu'issu de la loi relative au renseignement

VI. En quatrième lieu, les associations exposantes entendent faire valoir, à titre complémentaire, que les dispositions du décret n° 2015-1185 sont illégales en l'absence de toute base juridique qui en permettent l'édiction, compte tenu de la contrariété de l'article 323-8 du code pénal – que les dispositions règlementaires attaquées mettent notamment en œuvre – avec des engagements internationaux de la France dont la Convention de Budapest sur la cybercriminalité, la Convention européenne des droits de l'homme et la Charte des droits fondamentaux de l'Union européenne.

VII. D'emblée, et <u>à titre liminaire</u>, il importe de relever que la loi n° 2015-912 du 24 juillet 2015 relative au renseignement a créé, par son article 18, une exception au droit pénal en faveur des agents des services spécialisés de renseignement désignés par le décret n° 2015-1185 attaqué.

VII-1 Codifié à l'article 323-8 du code pénal, ce texte dispose que :

« *Le présent chapitre [sur les atteintes aux systèmes de traitement automatisé de données, dits « **STAD** »] n'est pas applicable aux mesures mises en œuvre, par les agents habilités des services de l'État désignés par arrêté du Premier ministre parmi les services spécialisés de renseignement mentionnés à l'article L. 811-2 du code de la sécurité intérieure, pour assurer hors du territoire national la protection des intérêts fondamentaux de la Nation mentionnés à l'article L. 811-3 du même code* ».

D'après l'étude d'impact du 18 mars 2015 du projet de loi relatif au renseignement – qui emploie à cet égard le terme d'« excuse pénale » – , cette disposition répondrait à la nécessité « *de protéger les agents qui mènent, notamment depuis le territoire national et donc directement passibles de la loi pénale française, des actions plus intrusives sur les systèmes d'information d'entité menaçant nos intérêts et localisés à l'étranger* » (**Prod. 1**).

Toutefois, force est de constater que le critère de localisation à l'étranger des systèmes de traitement automatisé de données ciblés n'a pas été retenu par le législateur et que seul le critère relatif à l'objectif d'« *assurer hors du territoire national la protection des intérêts fondamentaux de la Nation* » est inscrit dans la loi.

VII-2 L'introduction de ces dispositions au sein du code pénal confère une forme d'impunité pour les agents des services spécialisés, qui les protège lorsqu'ils mènent des actions portant atteinte à des systèmes de traitement automatisé de données (« STAD ») et cela, même si les

opérations visent des personnes ou équipements localisés ou rattachables au territoire national.

En effet, en l'absence de toute précision, l'objectif d'« *assurer hors du territoire national la protection des intérêts fondamentaux de la Nation* » ne peut en en aucun cas :

- Être distingué de la protection classique des intérêts fondamentaux de la Nation, soit une notion dont le caractère indéterminé a déjà été mis en avant par les parties requérantes ;
- Assurer une protection différenciée des ressortissants nationaux ou étrangers ou encore des personnes situées ou non sur le territoire national ;
- Prévenir une atteinte aux ressortissants ou équipements nationaux.

Pour comprendre la portée matérielle de cette immunité, il importe de préciser que le champ des actions des services de renseignement sur les systèmes de traitement automatisé de données couvertes par l'immunité offerte par l'article 323-8 du code pénal concernent notamment les faits de :

- Accéder ou se maintenir frauduleusement dans un système de traitement automatisé de données ;
- Entraver le fonctionnement d'un système de traitement automatisé de données ;
- Introduire, extraire, transmettre, modifier, supprimer frauduleusement des données stockées dans un système de traitement automatisé de données ;
- Importer, détenir, offrir, céder ou mettre à disposition un équipement, un instrument, un programme informatique ou toute donnée conçus ou spécialement adaptés pour commettre un ou plusieurs des faits précédents, sans motif légitime, notamment de recherche ou de sécurité informatique.

VII-3 En somme, l'article 323-8 du code pénal permet aux agents des services spécialisés d'être protégés pénalement en cas d'opérations de piratage d'un système de traitement automatisé de données ou en cas d'échange de données, de logiciels ou d'équipements adaptés pour le

piratage d'un système de traitement automatisé de données, quel que soit le lieu de cette opération, la nationalité ou le lieu de résidence des personnes visées, et ce compte tenu de la très grande variété des pratiques mises en œuvre.

Concrètement, cette disposition protège les agents des services concernant des opérations courantes de piratage ou de transfert national et international de moyens de piratage, tels que des failles de sécurité non-dévoilées (dites failles « *zero day* ») ou des logiciels exploitant des vulnérabilités dans les programmes informatiques — appelés « exploits ».

Ces dernières années ont d'ailleurs été riches en révélations importantes concernant les opérations de piratage et la conception, l'importation et l'exportation de moyens de piratage par les services de renseignement.

VII-3.1 À l'étranger, l'exemple du « malware » (programme malveillant) Stuxnet est parlant. Ce programme, principalement réalisé par les services américains et israéliens, visait à physiquement endommager des centrifugeuses nucléaires iraniennes. Stuxnet remplaçait les ordres donnés par le programme de contrôle par défaut par des ordres poussant les centrifugeuses à leur limite critique de rotation. Stuxnet a endommagé un cinquième du parc d'enrichissement d'uranium iranien.

Les concepteurs ont cependant perdu le contrôle de ce *malware*, au point que le virus a fini par infecter de nombreux systèmes informatiques dans le monde entier, notamment des systèmes américains et des systèmes de contrôle du secteur privé, comme des banques (ZETTER Kim, « Countdown to zerodays », Crown Publishers New York, 2014, pages 894-895, p. 900).

Le lancement du logiciel malveillant Stuxnet en 2007 a marqué un tournant dans l'histoire des logiciels malveillants développés par des services de renseignement (FINKLE Jim, « *Researchers say Stuxnet was deployed against Iran in 2007*», Reuters, 26 February 2013).

En effet, il est le premier à avoir eu pour **objectif de porter atteinte à des infrastructures critiques et des organismes d'importance vitale**, en sabotant le fonctionnement des systèmes de contrôle des

centrifugeuses fabriqués par Siemens et utilisés pour l'enrichissement d'uranium de la centrale de Natanz, afin d'endommager physiquement les équipements iraniens et ainsi ralentir le développement du nucléaire dans ce pays.

L'attaque du logiciel de rançon « WannaCrypt » à partir du 12 mai 2017 est par ailleurs un exemple idoine de la vitesse à laquelle un outil développé par les services de renseignement d'un pays pour exploiter les failles de programmes utilisés dans le monde entier peut être détourné par des groupes malintentionnés et causer des dommages considérables pour le secteur privé et la population. Cela, alors même que la vulnérabilité technique avait entre-temps été corrigée par Microsoft. L'attaque de WannaCrypt a par exemple perturbé le fonctionnement de plus de 45 hôpitaux publics en Angleterre et le déroulement de la production d'usines Renault en France.

Ainsi, depuis le lancement de Stuxnet en 2007, de nombreux logiciels malveillants obtenus ou développés par les services de renseignement ont eu pour objet de porter atteinte à des équipements informatisés — opérations qui relèvent de la qualification du chapitre III du titre II du livre III du code pénal.

VII-3.2 En France, loin d'être abstraites, les mesures pour lesquelles les agents bénéficient désormais d'une impunité étaient en réalité déjà pratiquées auparavant par les services français, comme le montre l'exemple du logiciel espion Babar utilisé entre 2011 et 2013 par la Ferme des animaux, un groupe étatique que les services canadiens soupçonnent d'être français (**Prod. 2**)

Comme l'explique la société Kaspersky, référence mondiale en matière de cybersécurité et d'analyse de logiciels espions, ce logiciel est une plateforme d'espionnage, ciblant entres autres des organisations gouvernementales, des entreprises du secteur privé, des journalistes, des activistes ou encore des organisations humanitaires (**Prod. 3**).

Elle se fait en deux temps.

Les services infectent un équipement visé. Si cet équipement semble être celui recherché, un programme y est alors injecté, pour permettre d'y installer Babar.

Cette plateforme d'espionnage permet alors d'intercepter les conversations opérées par le biais de plateformes de communication telles que Skype, MSN ou Yahoo Messenger.

Elle permet aussi d'enregistrer les mots et codes d'accès rédigés sur un clavier d'ordinateur (par *keyloggers*), de surveiller la navigation en ligne de la victime en extrayant des preuves de la navigation, et elle a été utilisée pour espionner plusieurs centres de recherches nucléaire iraniens, des universités et des institutions financières européennes (**Prod. 4**).

Ces pratiques attentatoires aux systèmes de traitement automatisé de données — dont les effets économiques sont importants — peuvent désormais, en application de l'article 323-8 du code pénal, être mises en œuvre par les agents des services de renseignement en toute impunité.

VII-4 Dans ce contexte, les associations entendent faire valoir que la méconnaissance par l'article 323-8 du code pénal, tel qu'issu de la loi relative au renseignement, des engagements internationaux de la France, notamment ceux applicables en matière de cybercriminalité, est manifeste.

Or, une telle méconnaissance affecte directement la légalité du décret attaqué puisque celui-ci a notamment pour objet de mettre en œuvre ce dispositif légal.

En effet, le décret n° 2015-1185 du 28 septembre 2015 portant désignation des services spécialisés de renseignement établit précisément la liste des services habilités à mettre en œuvre les techniques de renseignement couvertes par l'article 18 de la loi renseignement devenu l'article 323-8 du code pénal.

Au demeurant, ces dernières dispositions prévoient explicitement que les mesures dont elles encadrent la mise en œuvre sont réalisées :

« *Par les agents habilités des services de l'État désignés par arrêté du Premier ministre* ***parmi les services spécialisés de renseignement mentionnés à l'article L. 811-2 du code de la sécurité intérieure*** ».

Quant à l'article L. 811-2, il renvoie lui-même au décret attaqué puisqu'il dispose que :

« *Les services spécialisés de renseignement sont désignés par décret en Conseil d'État. Ils ont pour missions, en France et à l'étranger, la recherche, la collecte, l'exploitation et la mise à disposition du Gouvernement des renseignements relatifs aux enjeux géopolitiques et stratégiques ainsi qu'aux menaces et aux risques susceptibles d'affecter la vie de la Nation. Ils contribuent à la connaissance et à l'anticipation de ces enjeux ainsi qu'à la prévention et à l'entrave de ces risques et de ces menaces* ».

VII-5 Par conséquent, le constat d'inconventionnalité de l'article 323-8 du code pénal privera, à ce titre, le décret attaqué de base légale.

Ce constat est inéluctable en ce que les dispositions litigieuses de l'article 323-8 du code pénal méconnaissent plusieurs séries d'engagements internationaux de la France.

Sur la violation de l'article 32 de la Convention de Budapest sur la cybercriminalité

VIII. Premièrement, les dispositions de l'article 323-8 du code pénal méconnaissent les exigences de l'article 32 de la Convention de Budapest.

VIII-1 En droit, cette Convention de Budapest stipule à son article 32(b) que :

« *Une Partie peut, sans l'autorisation d'une autre Partie, : […] b. accéder à, ou recevoir au moyen d'un système informatique situé sur son territoire, des données informatiques stockées situées dans un autre Etat,* ***si la Partie obtient le consentement légal et volontaire*** *de la personne légalement autorisée à lui divulguer ces données au moyen de ce système informatique* ».

Ainsi, en plus de conditionner l'accès ou la réception de données au consentement d'une personne y étant habilitée, cet article s'oppose à tout régime discriminatoire applicable à l'accès transfrontière aux données stockées sur des équipements situés à l'étranger vis-à-vis du régime prévalant sur le territoire national (**Prod. 5**).

Qui plus est, dans sa notice d'orientation du 8 décembre 2014 sur l'application de la Convention de Budapest, le comité de la convention cybercriminalité du Conseil de l'Europe établit clairement que « *dans tous les cas, les services répressifs doivent appliquer les mêmes normes juridiques dans l'application de l'article 32b que dans leur propre pays. Si l'accès aux données ou leur divulgation ne seraient pas autorisés sur le territoire national, il en va de même dans l'application de l'article 32b.* » (Comité de la Convention Cybercriminalité du Conseil de l'Europe, Notes d'orientation du T-CY adoptées par le T-CY lors des 8e, 9e et 12e réunions plénières, 8 décembre 2014, p. 25)

VIII-2 Or, en l'occurrence, l'article 323-8 du code pénal crée un régime dérogatoire à l'encadrement des atteintes portées aux systèmes de traitement automatisé de données dès lors que ces atteintes ont pour objet la mise en œuvre de mesures « *pour assurer hors du territoire national la protection des intérêts fondamentaux de la Nation* ».

Dès lors, les encadrements et les sanctions prévus par le code de la sécurité intérieure et le chapitre III du titre II du livre III du code pénal ne sont pas applicables si les agents des services désignés par le décret attaqué ont recours, sur le territoire national ou hors de celui-ci, à ces mesures dans l'objectif d'« *assurer hors du territoire national la protection des intérêts fondamentaux de la Nation* ».

De plus, le recours par les services spécialisés de renseignement aux atteintes aux systèmes de traitement automatisé de données pour assurer la protection des intérêts de la Nation hors du territoire national ne prévoit aucunement l'obtention d'un « *consentement légal et volontaire de la personne légalement autorisée à lui divulguer ces données au moyen de ce système informatique* ».

Au surplus, l'immunité pénale suppose qu'il n'y ait aucune procédure de contrôle prévue par la loi, puisque ni autorisation du Premier ministre, ni avis de la CNCTR ne sont prévus.

Ces actions intrusives se feraient donc sans consentement et en toute impunité.

Par conséquent, les dispositions de l'article 323-8 du code pénal méconnaissent directement l'article 32(b) de la Convention de Budapest.

De ce chef, l'annulation des dispositions attaquées du décret s'impose faute de base légale.

Sur la violation de l'article 6 de la Convention de Budapest sur la cybercriminalité

IX. Deuxièmement, les dispositions de l'article 323-8 du code pénal méconnaissent également les exigences de l'article 6 de la même Convention de Budapest.

IX-1 En droit, l'article 6 « Abus de dispositifs » de la Convention de Budapest sur la cybercriminalité stipule que :

« *1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, lorsqu'elles sont commises intentionnellement et* ***sans droit*** *:*

a) la production, la vente, l'obtention pour utilisation, l'importation, la diffusion ou d'autres formes de mise à disposition:

i) d'un dispositif, y compris un programme informatique, principalement conçu ou adapté pour permettre la commission de l'une des infractions établies conformément aux articles 2 à 5 ci-dessus;

ii) d'un mot de passe, d'un code d'accès ou de données informatiques similaires permettant d'accéder à tout ou partie d'un système informatique, dans l'intention qu'ils soient utilisés afin de commettre l'une ou l'autre des infractions visées par les articles 2 à 5;

[…]

3. Chaque Partie peut se réserver le droit de ne pas appliquer le paragraphe 1 du présent article, à condition que cette réserve ne porte pas sur la vente, la distribution ou toute autre mise à disposition des éléments mentionnés au paragraphe 1.a.ii du présent article ».

À propos de ces stipulations, le Comité de la Convention Cybercriminalité a adopté la note suivante :

« *Les logiciels malveillants sont des dispositifs relevant de la définition figurant à l'article 6 (les Parties qui émettent des réserves quant à l'article 6 doivent néanmoins toujours ériger en infraction la vente, la distribution ou la mise à disposition des dispositifs visés par ledit article). Et ce parce qu'ils sont généralement conçus ou adaptés avant tout pour commettre les infractions visées aux articles 2 à 5. Par ailleurs, l'article érige en infraction pénale la vente, l'obtention pour utilisation, l'importation, la distribution ou d'autres formes de mise à disposition de mots de passe, de code d'accès ou de données similaires permettant de s'introduire dans des systèmes informatiques* » (**Prod. 5**).

Il en ressort que l'article 6 insiste de manière notable sur l'importance pour les parties à la Convention de Budapest d'ériger en infraction pénale « *la vente, la distribution ou toute autre mise à disposition des éléments mentionnés au paragraphe 1.a.ii du présent article* » tels que les logiciels malveillants ou les dispositifs logiciels conçus pour permettre les atteintes aux systèmes de traitement automatisé de données.

A cet égard, aucune réserve n'est permise par les parties à la Convention.

IX-2 En l'occurrence, l'article 323-8 précité permet aux agents des services spécialisés de renseignement de bénéficier d'une forme

d'impunité pour des infractions relevant de l'article 323-3-1 du code pénal, lequel prévoit que :

« *Le fait, sans motif légitime, notamment de recherche ou de sécurité informatique, d'importer, de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou toute donnée conçus ou spécialement adaptés pour commettre une ou plusieurs des infractions prévues par les articles 323-1 à 323-3 est puni des peines prévues respectivement pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée* ».

Cette disposition porte sur les échanges de logiciels malveillants et d'autres moyens de piratage de systèmes ou de réseaux entiers.

Or, ces échanges ne sont pas encadrés par les règles applicables aux techniques de renseignement prévues par le code de la sécurité intérieure (concernant la fixation d'une limite à la durée de l'exécution de la mesure, une procédure d'analyse, d'utilisation et de conservation des données, des précautions de transfert des données et les conditions d'effacement ou de destruction des données, etc.).

Ces opérations sont donc effectuées **intentionnellement et sans droit**, et, dès lors, doivent faire l'objet — sans dérogation — d'une infraction pénale en droit français.

Afin d'assurer que la production, la vente, l'obtention pour utilisation, l'importation, la diffusion ou d'autres formes de mise à disposition de données informatiques pour assurer hors du territoire national la protection des intérêts fondamentaux de la Nation ne soient pas faits « sans droit », le recours à ces opérations doit être encadré par la loi et, ses abus faire l'objet d'une sanction.

Par conséquent, l'article 323-8 du code pénal méconnait également l'article 6 de la Convention de Budapest.

De ce chef encore, l'annulation des dispositions du décret litigieux s'impose également, toujours faute de base légale.

Sur la violation des articles 8 et 13 de la Convention européenne des droits de l'homme

X. Troisièmement, les dispositions de l'article 323-8 du code pénal méconnaissent aussi les exigences des articles 8 et 13 de la Convention européenne des droits de l'homme

Et ce, à deux titres.

Sur l'insuffisant encadrement légal des opérations des agents de services de renseignement

XI. D'une part, l'insuffisance des garanties susceptibles d'encadrer les opérations des agents de services de renseignement visées à l'article 323-8 du code pénal méconnait les exigences conventionnelles.

XI-1 En droit, l'article 8 de la Convention européenne des droits de l'homme prévoit 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 ».

Par ailleurs, il résulte de l'article 13 de la Convention européenne des droits de l'homme que :

« *Toute personne dont les droits et libertés reconnus dans la présente Convention ont été violés, a droit à l'octroi d'un recours effectif devant une instance nationale, alors même que la violation aurait été commise par des personnes agissant dans l'exercice de leurs fonctions officielles* ».

Ainsi, et au terme de ces stipulations, la Cour européenne des droits de l'homme a imposé que l'autorité publique encadre l'étendue et les modalités de son appréciation de la pertinence du recours aux moyens de surveillance en énonçant que :

« *76. La Cour rappelle sa jurisprudence constante selon laquelle* ***les termes « prévue par la loi » signifient que la mesure litigieuse doit avoir une base en droit interne et être compatible avec la prééminence du droit****, expressément mentionnée dans le préambule de la Convention et inhérente à l'objet et au but de l'article 8 de la Convention. La loi doit donc être suffisamment accessible et* ***prévisible****, c'est-à-dire énoncée avec assez de précision pour permettre au justiciable – en s'entourant au besoin de conseils éclairés – de régler sa conduite (S. et Marper c. Royaume-Uni [GC], nos 30562/04 et 30566/04, §§ 95-96, CEDH 2008).*

« 77. Pour répondre à ces exigences, ***le droit interne doit offrir une certaine protection contre les atteintes arbitraires des pouvoirs publics*** *aux droits garantis par la Convention. Lorsqu'il s'agit de questions touchant aux droits fondamentaux, la loi irait à l'encontre de la prééminence du droit, l'un des principes fondamentaux d'une société démocratique consacrés par la Convention, si le pouvoir d'appréciation accordé à l'exécutif ne connaissait pas de limite. En conséquence,* ***elle doit définir l'étendue et les modalités d'exercice d'un tel pouvoir avec une netteté suffisante*** *(Rotaru c. Roumanie [GC], no 28341/95, § 55, CEDH 2000Ici commence la citation) […]* » (Cour EDH, 4e sect, 12 janv. 2010, *Gillan c. Royaume-Uni*, no 4158/05).

En outre, l'effectivité du droit à la protection des données à caractère personnel implique l'obligation pour les autorités nationales de sanctionner toute atteinte à ce droit, notamment par la voie pénale.
En effet, une telle obligation de sanction des atteintes au droit au respect de la vie privée peut être dérivée de l'article 8 de la Convention européenne des droits de l'homme.

Ainsi, selon une jurisprudence solennelle et désormais constante, la Cour juge 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 s'ajoutent des obligations positives inhérentes à un respect effectif de la vie privée ou familiale. Elles peuvent impliquer l'adoption de mesures visant au respect de la vie privée jusque dans les relations des individus entre eux » (Cour EDH, G.C. 12 nov. 2013, *Söderman c. Suède*, Req. n° 5786/08, § 78).

Or, *« lorsqu'un aspect particulièrement important de l'existence ou de l'identité d'un individu se trouve en jeu, ou que les activités en cause concernent un aspect des plus intimes de la vie privée […] la marge laissée à l'Etat est d'autant plus restreinte* » (*Ibid.* § 79).

Au surplus, et corrélativement, l'obligation positive de protection dérivée de l'article 8 peut impliquer que « *les Etats membres […] se dot[ent] de dispositions pénales efficaces* » (*Ibid*. § 82 ; v. aussi Cour EDH, G.C. 28 janvier 2014, *O'Keefe c. Irlande*, Req. n° 35810/09).

XI-2 En l'espèce, l'article 323-8 du code pénal autorise la mise en place de mesures d'atteinte aux systèmes de traitement automatisé de données sans prévoir de garanties particulières en matière de données personnelles.

L'interprétation de l'article 8 par les juges emporte par ailleurs une obligation positive pour la France d'encadrer pénalement les opérations visées par l'article 323-8.

La Cour européenne des droits de l'homme a précisé les critères que la loi doit nécessairement prévoir pour encadrer la mise en place de mesures de surveillance :

« *95. Dans sa jurisprudence relative aux mesures de surveillance secrète, la Cour énonce les* ***garanties minimales*** *suivantes contre les abus de pouvoir que la loi doit renfermer :*

- *La nature des infractions susceptibles de donner lieu à un mandat d'interception ;*
- *La définition des catégories de personnes susceptibles d'être mises sur écoute ;*
- *La* ***fixation d'une limite à la durée de l'exécution de la mesure*** *;*
- *La* ***procédure à suivre pour l'examen, l'utilisation et la conservation des données recueillies***

- *Les précautions à prendre pour la communication des données à d'autres parties*
- *Les* ***circonstances dans lesquelles peut ou doit s'opérer l'effacement ou la destruction des enregistrements*** » (Cour EDH, 3e sect., 29 juin 2006, *Weber c. Allemagne*, Req. no 54934/00)

Ces critères sont applicables *mutatis mutandis* à des faits d'atteintes aux systèmes de traitement automatisé de données.

En effet, dans le cadre de son arrêt *RE c. Royaume-Uni* relatif à une affaire de surveillance sous couverture, la Cour européenne des droits de l'homme a pris une position à portée générale en déclarant que :

« [L]e facteur décisif sera le niveau d'atteinte porté au droit à la vie privée de la personne et non la définition technique de cette atteinte ») (Cour EDH, 4e sect., 25 oct. 2015, *R.E. c. Royaume-Uni*, no 62498/11, § 130 : *Traduction libre de l'anglais :* "*[T]he decisive factor will be the level of interference with an individual's right to respect for his or her private life and not the technical definition of that interference"*)

Par ailleurs, l'arrêt *Kennedy* a permis à la Cour de mettre en lumière que l'absence de recours effectif appelle un contrôle accru :

« *Lorsqu'il n'existe aucune possibilité de contester l'application de mesures de surveillance secrète au niveau interne, les soupçons et les craintes de la population quant à l'usage abusif qui pourrait être fait des pouvoirs de surveillance secrète ne sont pas injustifiés. En pareil cas, un contrôle accru par la Cour s'avère nécessaire même si, en pratique, le risque de surveillance n'est guère élevé* » (Cour EDH, 4e sect., 18 mai 2010, *Kennedy c. Royaume-Uni*, no 26839/05, § 124)

Cette jurisprudence peut être utilement rapprochée de l'arrêt *Pruteanu*, qui précise quant à lui l'interprétation par la Cour de ce qu'est un contrôle effectif et qui l'associe à l'article 8 de la Convention européenne des droits de l'homme :

« *48. De même, quel que soit le système de surveillance retenu,* ***la Cour doit se convaincre de l'existence de garanties adéquates et suffisantes contre les abus****. Cette appréciation ne revêt qu'un caractère relatif, elle dépend,* ***entre autres****, du* ***type de recours fourni par le droit interne****.*

Par conséquent, il y a lieu de rechercher si les procédures destinées au contrôle de l'adoption et de l'application des mesures restrictives ***sont aptes à limiter à ce qui est nécessaire dans une société démocratique*** *l'ingérence résultant de la législation incriminée (Klass et autres c. Allemagne, 6 septembre 1978, § 50 et suiv., série A no 28). […]*

55. En ce qui concerne la voie de l'action civile en dédommagement indiquée par le Gouvernement, la Cour relève qu'en effet la Convention est directement applicable en Roumanie et qu'elle l'emporte sur les dispositions du droit national qui seraient en contradiction avec elle (paragraphe 26 ci‑dessus ; voir, mutatis mutandis, Abramiuc c. Roumanie, no 37411/02, § 125, 24 février 2009).

Cependant, en l'espèce, ***le Gouvernement n'a fourni aucun exemple de jurisprudence qui démontrerait l'effectivité de cette voie de recours*** *(Rachevi c. Bulgarie, no 47877/99, § 64, 23 septembre 2004).*

De plus, un recours devant le juge civil pour une mise en cause de la responsabilité de l'État, de nature indemnitaire, ***ne serait pas de nature à permettre la réalisation d'un contrôle de la légalité des enregistrements litigieux*** *et à aboutir, le cas échéant, à une décision ordonnant la destruction de ceux-ci – résultat recherché par le requérant –, de sorte que l'****on ne peut y voir un « contrôle efficace » aux fins de l'article 8 de la Convention*** *(voir, mutatis mutandis, Xavier Da Silveira, précité, § 48) […]*

56. Dès lors, compte tenu de ce qui précède, la Cour estime que l'ingérence litigieuse était, dans les circonstances de l'espèce, disproportionnée par rapport au but visé et que, par conséquent, ***l'intéressé n'a pas bénéficié du « contrôle efficace » requis par la prééminence du droit et apte à limiter l'ingérence à ce qui était « nécessaire dans une société démocratique*** » (Coure EDH, 3e sect., 3 févr. 2015, *Pruteanu c. Roumanie*, no 30181/05, § 48, 55, 56)

XI-3 Or, les dispositions de l'article 323-8 du code pénal ne répondent pas aux exigences énoncées par la Cour européenne des droits de l'homme lorsque, pour assurer hors du territoire national la protection des intérêts fondamentaux de la Nation, les agents opèrent des transferts de moyens d'atteinte aux systèmes de traitement automatisé de données.

XI-3.1 D'emblée, il convient de rappeler combien les hypothèses de transferts de moyens d'atteinte aux systèmes de traitement automatisé de données par les services peuvent emporter de graves conséquences si lesdits moyens d'atteintes venaient à être volés ou détournés.

L'exemple déjà précédemment évoqué de Stuxnet l'illustre amplement.

Sa modification ultérieure par les services israéliens pour un second lancement a échoué, en ce sens que le programme a infecté des systèmes dans le monde entier plutôt que de se cantonner aux systèmes iraniens visés. Si les transferts de données de programmes informatiques avaient été mieux encadrés entre les États-Unis et Israël, les États-Unis n'auraient auraient peut-être évité de s'impliquer dans ces transferts en collaboration avec Israël, ce qui aurait épargné à son secteur privé et à son administration d'être frappés par l'infection de 2010 (Article de l'équipe américaine de réponse aux urgences informatiques (ICS-CERT), 15 septembre 2010. Disponible en ligne : <https://ics-cert.us-cert.gov/advisories/ICSA-10-238-01B>).

D'où l'importance cruciale de prévoir toutes « *les précautions à prendre pour la communication des données à d'autres parties* » (Cour EDH, 3e sect., 29 juin 2006, *Weber c. Allemagne*, no 54934/00, § 95).

XI-3.2 Or, les dispositions de l'article 323-8 du code pénal méconnaissent directement l'impératif de protection contre les atteintes arbitraires des pouvoirs publics, tel que notamment précisé par l'arrêt *Gillan* (cf. *supra* Cour EDH, 4e sect, 12 janv. 2010, *Gillan c. Royaume-Uni*, no 4158/05, § 76 et 77).

En témoigne ainsi le mutisme total de l'article 323-8 concernant les abus possibles du recours à cet article.

En outre, il importe de relever que l'article 323-8 du code pénal autorise la mise en place de mesures d'atteinte aux systèmes de traitement automatisé de données sans prévoir les garanties minimales pour les encadrer.

Partant, aucune des deux premières garanties énoncées au paragraphe 95 de la décision *Weber* n'est respectée de manière satisfaisante par le code de la sécurité intérieure.

S'agissant des quatre suivantes imposant la fixation d'une limite à la durée de l'exécution de la mesure, une procédure d'analyse, d'utilisation et de conservation des données, des précautions de transfert des données et les conditions d'effacement ou de destruction des données, aucune d'elles n'est prévue pour encadrer le recours par les services à l'article 323-8 du code pénal.

Les juges de la Cour européenne des droits de l'homme les ont pourtant énoncées comme de simples « garanties minimales » d'une surveillance secrète mise en place dans une société démocratique.

L'atteinte aux données personnelles des ressortissants européens et français visés par ces mesures est donc patente.

XI-3.3 Par ailleurs, les voies de recours offertes aux victimes d'éventuels abus des techniques extrêmement intrusives que permet l'article 323-8 du code pénal sont insuffisantes.

Par contraste avec une interception ponctuelle de communications ou la fouille d'un appartement, l'exploitation de failles dans l'équipement informatique d'une personne physique ou morale permet à l'intéressé de contrôler et d'accéder de façon illimitée à une quantité pléthorique de données confidentielles, voire personnelles et sans lien aucun avec les suspicions ayant amené les services à envisager une mesure aussi intrusive.

Pourtant, en dépit de la gravité des opérations ainsi permises, le législateur n'a prévu aucune voie de recours spécifique au profit des victimes directes ou indirectes du développement ou du transfert de moyens de piratage par les services de renseignement français.

Tout au plus un engagement au titre de la responsabilité est envisageable.

Mais s'agissant d'une opération par définition secrète, il sera pour le moins difficile de prouver un lien de causalité entre cette opération de

piratage ou d'échange de moyens de piratage et le dommage subi par la victime.

Dès lors, non seulement les victimes d'atteinte aux systèmes de traitement automatisé de données ne peuvent défendre leur droit à la vie privée et à la protection des données personnelles que lorsqu'elles peuvent prouver que l'atteinte à ces principes a été tellement importante qu'ils en ont souffert des dommages quantifiables ou probants.

Mais en outre, puisque le piratage a pour objet de porter atteinte aux programmes d'un équipement ou un équipement lui-même, sans laisser de traces, imposer à une victime d'abus de cette technique de renseignement éminemment intrusive d'apporter la preuve du recours à ces moyens revient à faire peser sur elle une charge radicalement excessive.

XI-3.4 Par conséquent, faute de garanties aptes à limiter à ce qui est nécessaire dans une société démocratique l'ingérence résultant des opérations des agents de services de renseignement, la dérogation prévue à l'article 323-8 du code pénal méconnait les exigences de la Convention européenne des droits de l'homme.

Mais il y a plus.

Sur l'insuffisant encadrement légal des échanges de données avec les services étrangers

XII. D'autre part, l'insuffisance des garanties susceptibles d'encadrer les échanges de données avec les services étrangers prévus à l'article 323-8 du code pénal méconnait tout autant les exigences conventionnelles.

XII-1 En droit, la Cour européenne des droits de l'homme juge qu'en matière de mesure de surveillance secrète des communications, conformément au principe de prééminence du droit, les Etats doivent limiter et tracer avec netteté les modalités d'exercice d'un tel pouvoir pour accorder à l'individu une protection satisfaisant les exigences de l'article 8 de la Convention européenne des droits de l'homme.

A ce titre, la Cour rappelle précisément les « garanties minimales contre les abus de pouvoir que la loi doit renfermer » dans son arrêt *Weber* :

« *[L]a nature des infractions susceptibles de donner lieu à un mandat d'interception, la définition des catégories de personnes susceptibles d'être mises sur écoute, la fixation d'une limite à la durée de l'exécution de la mesure, la procédure à suivre pour l'examen, l'utilisation et la conservation des données recueillies, les précautions à prendre pour la communication des données à d'autres parties, et les circonstances dans lesquelles peut ou doit s'opérer l'effacement ou la destruction des enregistrements (voir, notamment, Huvig, précité, § 34, Amann, précité, § 76, Valenzuela Contreras, précité, § 46, et Prado Bugallo c. Espagne, no 58496/00, § 30, 18 février 2003)* » (Cour EDH, 3e sect., 29 juin 2006, *Weber c. Allemagne*, Req. no 54934/00, § 95).

XII-2 En l'occurrence, l'article L. 833-2 du code de la sécurité intérieure dispose, en son 4°, que :

« *Pour l'accomplissement de ses missions, la commission […] peut solliciter du Premier ministre tous les éléments nécessaires à l'accomplissement de ses missions, y compris lorsque la technique de recueil de renseignement mise en œuvre n'a fait l'objet ni d'une demande, ni d'une autorisation ou ne répond pas aux conditions de traçabilité,* ***à l'exclusion des éléments communiqués par des services étrangers ou par des organismes internationaux*** ».

Or, aucune disposition légale ne définit les finalités ou encore le champ des renseignements recueillis par l'intermédiaire des services étrangers et transmis aux autorités nationales.

Les dispositions litigieuses ne prévoient pas davantage la durée de conservation de ces données, ou les modalités dans lesquelles leur effacement ou destruction peuvent s'opérer.

Enfin, ni les précautions à prendre, ni même la procédure à suivre pour la communication à d'autres parties des données ainsi récoltées ne sont prévues.

Or, ainsi que cela a été précisé par les associations exposantes, l'absence de toute garantie en matière de recueil de renseignements

auprès de services étrangers – combinée aux très faibles garanties qui entourent l'interception par les services français de communications internationales – revient à autoriser les agences de renseignement en Europe, dont les services français, à contourner les contraintes légales prévues dans chaque État.

XII-3 Par conséquent, en renonçant à définir le champ matériel, personnel et temporel des renseignements transmis par les renseignements étrangers ainsi que les procédures de contrôle s'exerçant sur l'exploitation de ces données, le législateur n'a pas mis en place les « garanties minimales » exigées par la Convention européenne des droits de l'homme.

Partant, faute d'encadrement légal suffisant, l'article 323-8 du code pénal méconnait les articles 8 et 13 de la Convention.

De ce chef, l'annulation des dispositions du décret litigieux s'impose là encore, à nouveau faute de base légale.

Sur la méconnaissance de l'article 1er protocole à la Convention européenne des droits de l'homme.

XIII. Quatrièmement, les dispositions de l'article 323-8 du code pénal méconnaissent aussi les exigences l'article 1er du protocole additionnel à la Convention européenne des droits de l'homme.

Et ce, à deux titres.

Sur l'interdiction de porter atteinte aux biens

XIII-1 En droit, il convient de rappeler que selon les stipulations de l'article 1er du premier protocole à la Convention européenne :

« Toute personne physique ou morale a droit au respect de ses biens. Nul ne peut être privé de sa propriété que pour cause d'utilité publique et dans les conditions prévues par la loi et les principes généraux du droit international.

Les dispositions précédentes ne portent pas atteinte au droit que possèdent les Etats de mettre en vigueur les lois qu'ils jugent nécessaires pour réglementer l'usage des biens conformément à l'intérêt général ou pour assurer le paiement des impôts ou d'autres contributions ou des amendes. »

Dans son arrêt de Grande Chambre *Centro Europa 7 SRL et Di Stefano c. Italie*, notamment, la Cour a interprété l'article 1 du Protocole n° 1 comme contenant « *trois normes distinctes : « la première, qui s'exprime dans la première phrase du premier alinéa et revêt un caractère général, énonce le principe du respect de la propriété ; la deuxième, figurant dans la seconde phrase du même alinéa, vise la privation de propriété et la soumet à certaines conditions ; quant à la troisième, consignée dans le second alinéa, elle reconnaît aux Etats le pouvoir, entre autres, de réglementer l'usage des biens conformément à l'intérêt général (...) Il ne s'agit pas pour autant de règles dépourvues de rapport entre elles. La deuxième et la troisième ont trait à des exemples particuliers d'atteintes au droit de propriété ; dès lors, elles doivent s'interpréter à la lumière du principe consacré par la première » »* (Cour EDH, G.C., 7 juin 2012, *Centro Europa 7 SRL et Di Stefano c. Italie,* Req. n° 38433/09, § 185).

Partant, *« cette disposition exige, avant tout et surtout, qu'une ingérence de l'autorité publique dans la jouissance du droit au respect des biens soit légale ». « Le principe de légalité présuppose également que les dispositions pertinentes du droit interne soient suffisamment accessibles, précises et prévisibles dans leur application (voir, mutatis mutandis, Broniowski précité, § 147) »* (*Ibid.*, § 187).

Par ailleurs, la Cour européenne a aussi jugé dans l'arrêt *Lallement c. France « qu'une mesure d'ingérence dans le droit au respect des biens [...] doit ménager* ***un « juste équilibre »*** *entre les exigences de l'intérêt général de la Communauté et les impératifs de la sauvegarde des droits fondamentaux de l'individu. En particulier, il doit exister un rapport raisonnable de proportionnalité entre les moyens employés et le but visé par toute mesure privant une personne de sa propriété »* (Cour EDH, 3e sect., 11 avril 2002, *Lallement c. France,* Req. n° 46044/99, § 18).

XIII-2 En l'espèce, et d'emblée, il importe de relever que les fournisseurs d'accès internet – parmi lesquels figurent d'ailleurs French Data Network (FDN) et les membres de la Fédération FDN (FFDN), requérants – sont propriétaires d'équipements informatiques qu'ils utilisent pour fournir les services auxquels ont souscrit leurs adhérents.

Autrement dit, ces personnes morales existent grâce à la vente d'abonnements payés par leurs adhérents, en échange des services liés à leurs équipements informatiques.

Or, en prévoyant que les agents des services spécialisés ne peuvent faire l'objet de poursuites pénales en cas d'opérations de piratage d'un système de traitement automatisé de données ou en cas d'échange de données, de logiciels ou d'équipements adaptés pour le piratage d'un système de traitement automatisé de données, les dispositions de l'article 323-8 du code pénal ont nécessairement ouvert la voie à des atteintes aux biens des fournisseurs d'accès.

Plus encore, tout autre propriétaire – personne physique ou morale – de données ainsi susceptibles d'être visées par de telles opérations peuvent subir une même atteinte.

En effet, il y a lieu de rappeler que ces atteintes aux systèmes de traitement automatisé de données (« STAD ») reviennent à porter atteinte non seulement aux programmes informatiques, mais également aux équipements informatiques eux-mêmes (cf. § 32 du témoignage de M. E. King pour Privacy International, novembre 2015. Disponible en ligne :
<https://www.privacyinternational.org/sites/default/files/Witness_Statement_Of_Eric_King.pdf>.).

Les atteintes aux STAD peuvent ainsi considérablement et durablement altérer le matériel physique et logiciel possédé par les requérantes, ce qui affecte inéluctablement leurs activités et intérêts économiques.

Pourtant, l'atteinte ainsi permise n'est encadrée par strictement aucune garantie légale, notamment en ce que l'activité des agents des services spécialisés n'est absolument pas soumise à un contrôle de la CNCTR.

De ce seul fait, l'atteinte ainsi portée au droit au respect des biens ne saurait prétendre à l'exigence de base légale ou encore de « *rapport raisonnable de proportionnalité* ».

Mais il y a plus.

Sur l'obligation positive de protection des biens

XIII-3 En droit, dans son arrêt *Tunnel Report Limited c. France* la Cour européenne a réaffirmé que *« l'article 1 du Protocole n° 1, qui tend pour l'essentiel à prémunir l'individu contre toute atteinte de l'Etat au respect de ses biens, peut également impliquer des obligations positives entraînant pour l'Etat certaines mesures nécessaires pour protéger le droit de propriété, notamment là où il existe un lien direct entre les mesures qu'un requérant pourrait légitimement attendre des autorités et la jouissance effective par ce dernier de ses biens*.

[...]

Pour apprécier la conformité de la conduite de l'Etat à l'article 1 du Protocole n° 1, la Cour doit se livrer à un examen global des divers intérêts en jeu, en gardant à l'esprit que la Convention a pour but de sauvegarder des droits qui sont « concrets et effectifs ». Elle doit aller au-delà des apparences et rechercher la réalité de la situation litigieuse. Cette appréciation peut porter [...] sur la conduite des parties, y compris les moyens employés par l'Etat et leur mise en œuvre. ***A cet égard, il faut souligner que l'incertitude – qu'elle soit législative, administrative, ou tenant aux pratiques appliquées par les autorités – est un facteur qu'il faut prendre en compte pour apprécier la conduite de l'Etat.*** *[...] »* (Cour EDH, 5e sect., *Tunnel Report Limited c. France*, Req. n° 27940/07, § 36 et 39).

XIII-4 En l'espèce, et ainsi que cela a déjà été souligné, il est manifeste que les dispositions litigieuses ont manqué de prévoir des garanties suffisantes pour satisfaire à l'obligation positive de protection du droit au respect des biens.

La méconnaissance des exigences de la Convention européenne est donc patente.

Partant, l'article 323-8 du code pénal méconnait aussi l'article 1er du Protocole 1 à la Convention européenne des droits de l'homme.

De ce chef enfin, l'annulation des dispositions du décret litigieux s'impose, là encore faute de base légale.

PAR CES MOTIFS, et tous autres à produire, déduire, suppléer, au besoin même d'office, les associations exposantes persistent dans les conclusions de leurs précédentes écritures.

SPINOSI & SUREAU
SCP d'Avocat au Conseil d'État et à la Cour de cassation

Productions :

1. Projet de loi relatif au renseignement, étude d'impact, NOR : PRMX1504410L/Bleue-1, 18 mars 2015, *Assemblée Nationale*
2. M. Untersinger, « "La Ferme des animaux", concepteur de logiciels espions depuis au moins 2009 », *Le Monde*, 6 mars 2015.
3. Billet de l'équipe de recherche et d'analyse de la société Kaspersky, le 6 mars 2015 (Source : https://securelist.com/animals-in-the-apt-farm/69114/)
4. Billet de P. Paganini le 1er juillet 2015, membre de l'Agence européenne ENISA (European Union Agency for Network and Information Security – Source : https://securityaffairs.co/wordpress/38204/cyber-crime/dino-malware-animal-farm.html).
5. Comité de la Convention Cybercriminalité (T-CY), *Note d'orientation du n°3. Accès transfrontalier aux données (article 32)*, adoptée par la 12ème réunion plénière du T-CY (2-3 décembre 2014)