Alexis Fitzjean Ó Cobhthaigh
Avocat au bareau de Paris
5, rue Daunou, 75 002 Paris
afoc@afocavocat.eu
01 53 63 33 10

Conseil d'État
Section du contentieux

Recours en excès de pouvoir
Requête introductive d'instance

POUR

La Quadrature du Net, association régie par la loi du 1er juillet 1901 dont le siège social est situé au 60 rue des Orteaux à Paris (75020), enregistrée en préfecture de police de Paris sous le numéro W751218406, représentée par son président en exercice, M. Axel Simon, dûment habilité à agir en justice

Tel. : 06 73 60 88 43

Mail : `contact@laquadrature.net`

Franciliens.net, association régie par la loi du 1er juillet 1901 dont le siège social est situé au 64 rue de la Pompe à Paris (75116), enregistrée en préfecture de police de Paris sous le numéro W941006323, représentée par son président en exercice, M. Daniele Pitrolo, dûment habilité à agir en justice

Tel. : 06 16 95 03 95

Mail : `bureau@listes.franciliens.net`

Fédération des fournisseurs d'accès à Internet associatifs, dite Fédération FDN, fédération d'associations régie par la loi du 1er juillet 1901 dont le siège social est situé au 16 rue de Cachy à Amiens (80090), enregistrée en préfecture de la Somme sous le numéro W751210904, regroupant 29 fournisseurs d'accès associatifs français déclarés auprès de l'ARCEP, et un fournisseur d'accès associatif belge déclaré auprès du régulateur national, représentée par son co-président en exercice, M. Benjamin Bayart, dûment habilité à agir en justice

Tel. : 06 60 24 24 94

Mail : `contact@ffdn.org`

CONTRE

Le décret n° 2018-1136 du 13 décembre 2018 pris pour l'application de l'article L. 2321-2-1 du code de la défense et des articles L. 33-14 et L. 36-14 du code des postes et des communications électroniques

Les exposantes défèrent le décret attaqué à la censure du Conseil d'État et en requièrent l'annulation en tous les chefs leur faisant griefs, par la présente requête sommaire à l'appui de laquelle sera produit un mémoire complémentaire.

Table des matières

1 Faits

1 La loi n° 2018-607 du 13 juillet 2018 relative à la programmation militaire pour les années 2019 à 2025 et portant diverses dispositions intéressant la défense établit les objectifs de la politique de défense française pour les années 2019 à 2025. Son Chapitre III réunit les dispositions relatives à la cyberdéfense et notamment les articles 34 et 35, qui prévoient les dispositifs mettant en œuvre des marqueurs techniques aux fins de détecter des événements susceptibles d'affecter la sécurité des systèmes d'information de leurs abonnés.

2 Précisément, l'article 34 de cette loi de programmation introduit dans le code des postes et des communications électroniques un article L. 33-14 qui dispose :

> « Art. L. 33-14.-Pour les besoins de la sécurité et de la défense des systèmes d'information, les opérateurs de communications électroniques peuvent recourir, sur les réseaux de communications électroniques qu'ils exploitent, après en avoir informé l'autorité nationale de sécurité des systèmes d'information, à des dispositifs mettant en œuvre des marqueurs techniques aux seules fins de détecter des événements susceptibles d'affecter la sécurité des systèmes d'information de leurs abonnés. « A la demande de l'autorité nationale de sécurité des systèmes d'information, lorsque celle-ci a connaissance d'une menace susceptible de porter atteinte à la sécurité des systèmes d'information, les opérateurs de communications électroniques ayant mis en œuvre les dispositifs prévus au premier alinéa procèdent, aux fins de prévenir la menace, à leur exploitation, en recourant, le cas échéant, à des marqueurs techniques que cette autorité leur fournit. « Par dérogation au II de l'article L. 34-1, les opérateurs de communications électroniques sont autorisés à conserver, pour une durée maximale de six mois, les données techniques strictement nécessaires à la caractérisation d'un évènement détecté par les dispositifs mentionnés au premier alinéa du présent article. Les données recueillies dans le cadre de l'exploitation de ces dispositifs autres que celles directement utiles à la prévention et à la caractérisation des menaces sont immédiatement détruites. « Lorsque sont détectés des événements susceptibles d'affecter la sécurité des systèmes d'information, les opérateurs de communications électroniques en informent sans délai l'autorité nationale de sécurité des systèmes d'information. « A la demande de l'autorité nationale de sécurité des systèmes d'information, les opérateurs de communications électroniques informent leurs abonnés de la vulnérabilité de leurs systèmes d'information ou des atteintes qu'ils ont subies. [...] »

Cette disposition insère également dans le code de la défense l'article suivant :

> « Art. L. 2321-2-1.-Lorsqu'elle a connaissance d'une menace susceptible de porter atteinte à la sécurité des systèmes d'information des autorités publiques, des opérateurs mentionnés aux articles L. 1332-1 et L. 1332-2 ou des opérateurs mentionnés à l'article 5 de la loi n° 2018-133 du 26 février 2018 portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la sécurité, l'autorité nationale de sécurité des systèmes d'information peut mettre en œuvre, sur le réseau d'un opérateur de communications électroniques ou sur le système d'information d'une personne mentionnée aux 1 ou 2 du I de l'article

> 6 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, des dispositifs mettant en œuvre des marqueurs techniques aux seules fins de détecter des événements susceptibles d'affecter la sécurité des systèmes d'information des autorités publiques et opérateurs mentionnés aux articles L. 1332-1 et L. 1332-2 du présent code ou à l'article 5 de la loi n° 2018-133 du 26 février 2018 précitée. Ces dispositifs sont mis en œuvre pour la durée et dans la mesure strictement nécessaires à la caractérisation de la menace. « Les agents de l'autorité nationale de sécurité des systèmes d'information individuellement désignés et spécialement habilités sont autorisés, aux seules fins de prévenir et de caractériser la menace affectant les systèmes d'information des autorités publiques ou des opérateurs mentionnés aux articles L. 1332-1 et L. 1332-2 du présent code ou des opérateurs mentionnés à l'article 5 de la loi n° 2018-133 du 26 février 2018 précitée, à procéder au recueil et à l'analyse des seules données techniques pertinentes, à l'exclusion de toute autre exploitation. « Les données techniques recueillies directement par l'autorité nationale de sécurité des systèmes d'information en application du premier alinéa du présent article ou obtenues en application du deuxième alinéa de l'article L. 2321-3 ne peuvent être conservées plus de dix ans. « Les données recueillies autres que celles directement utiles à la prévention et à la caractérisation des menaces sont immédiatement détruites.[...]. »

3 L'essentiel des modalités d'application de ces dispositions sont renvoyées à un décret en Conseil d'État : le décret n° 2018-1136 du 13 décembre 2018 pris pour l'application de l'article L. 2321-2-1 du code de la défense et des articles L. 33-14 et L. 36-14 du code des postes et des communications électroniques.

4 C'est le décret présentement attaqué.

2 Sur l'intérêt à agir des requérantes

5 À titre liminaire, il importe de souligner que les associations exposantes sont bien recevables à solliciter l'annulation du décret pris pour l'application de l'article L. 2321-2-1 du code de la défense et des articles L. 33-14 et L. 36-14 du code des postes et des communications électroniques.

6 L'association « La Quadrature du Net », première exposante, a notamment pour objet, aux termes de l'article 3 de ses statuts constitutifs, « de mener une réflexion, des études, analyses, actions pour la défense des libertés individuelles sur Internet » et « d'encourager l'autonomie des usagers et leur prise de contrôle sur les données les concernant ».

7 L'association « Fédération des fournisseurs d'accès à Internet associatif » dite « Fédération FDN », deuxième exposante, regroupe et représente des fournisseurs d'accès à Internet, déclarés auprès du régulateur national (l'ARCEP, pour les 29 opérateurs de droit français) auxquels le décret attaqué est directement applicable. En cela, son intérêt à agir est incontestable. Par ailleurs, et au surplus, la Fédération FDN, ainsi que ses membres qui ont adhéré à ses statuts et à sa charte, a pour vocation, entre autres, de protéger les libertés liées à l'usage de la connexion à Internet fournie aux abonnés. Par exemple, au titre de la charte de la fédération « *Le fournisseur s'interdit de porter atteinte, en quoi que ce soit aux donnés transportées pour les abonné·e·s, sans l'accord de l'abonné·e concerné·e.* », ou encore « *Le fournisseur s'interdit de filtrer les accès Internet de ses abonné·e·s, sauf obligation légale stricte. Ces obligations légales, et les moyens techniques mis en œuvre pour les satisfaire, sont clairement indiqués à tous les membres, et donc tou·te·s les abonné·e·s du fournisseur.* ».

8 L'association « Franciliens.net », troisième exposante, est un fournisseur d'accès à Internet membre de la Fédération FDN. En tant qu'opérateur, son intérêt à agir est également incontestable.

3 Sur la légalité externe

3.1 En ce qui concerne le défaut de notification à la Commission européenne

9 **En premier lieu**, le décret attaqué a été pris au terme d'une procédure irrégulière en ce que son adoption n'a pas été précédée d'une notification à la Commission européenne.

10 **En droit**, la directive 2015/1535 du 9 septembre 2015, en son article 1er 1. b) définit la notion de « service de la société de l'information » comme :

> « tout service presté normalement contre rémunération, à distance, par voie électronique et à la demande individuelle d'un destinataire de services »

11 L'article 1er 1. e) définit la « règle relative aux services » comme :

> « une exigence de nature générale relative à l'accès aux activités de services au sens du point b) et à leur exercice, notamment les dispositions relatives au prestataire de services, aux services et au destinataire de services, à l'exclusion des règles qui ne visent pas spécifiquement les services définis audit point. »

12 L'article 1er 1. f) définit la « règle technique » comme :

> « une spécification technique ou autre exigence ou une règle relative aux services, y compris les dispositions administratives qui s'y appliquent, dont l'observation est obligatoire de jure ou de facto, pour la commercialisation, la prestation de services, l'établissement d'un opérateur de services ou l'utilisation dans un État membre ou dans une partie importante de cet État, de même que, sous réserve de celles visées à l'article 7, les dispositions législatives, réglementaires et administratives des États membres interdisant (...) de fournir ou d'utiliser un service ou de s'établir comme prestataire de services. »

13 **En l'espèce**, les mesures créées par le décret sont bien des règles techniques au sens de la directive. En effet, il s'agit bien de dispositions administratives dont l'observation est obligatoire et s'appliquant à des services tels que définis par la directive puisque sont notamment visés les hébergeurs, tels que définis à l'article 6, I, 1° de la LCEN et prestataires de services de la société de l'information par excellence.

14 Dès lors, le projet de décret devait être notifié à la Commission européenne, l'article 5 de la directive 2015/1535 disposant quant à lui que :

> « Sous réserve de l'article 7, les États membres communiquent immédiatement à la Commission tout projet de règle technique, sauf s'il s'agit d'une simple transposition intégrale d'une norme internationale ou européenne, auquel cas une simple information quant à la norme concernée suffit ; ils adressent également à la Commission une notification concernant les raisons pour lesquelles l'établissement d'une telle règle technique est nécessaire, à moins que ces raisons ne ressortent déjà du projet.»

15 Ne s'agissant ni d'un cas visé à l'article 7 ni d'une transposition intégrale d'une norme internationale ou européenne, le décret devait être notifié à la Commission européenne

conformément à la procédure établie par la directive 2015/1535. Cette interprétation de la directive 2015/1535 est d'ailleurs conforme à la solution adoptée par le Conseil d'État dans son arrêt du 10 juin 2013 rendu dans l'affaire n° 327.375.

16 **En conclusion**, le Gouvernement ayant manqué de le notifier à la Commission européenne, le décret attaqué n'a pas été adopté conformément aux dispositions susvisées de la directive 2015/1535 et doit donc être annulé.

3.2 En ce qui concerne le défaut d'étude d'impact

17 **En second lieu**, le décret attaqué a été pris au terme d'une procédure irrégulière en ce que son adoption n'a pas été précédée d'une étude d'impact.

18 **En droit**, en cas de traitement de données à caractère personnel mis en œuvre, à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, l'article 70-4 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés prévoit que :

> « Si le traitement est susceptible d'engendrer un risque élevé pour les droits et les libertés des personnes physiques, notamment parce qu'il porte sur des données mentionnées au I de l'article 8, le responsable de traitement effectue une analyse d'impact relative à la protection des données à caractère personnel.»

19 Les données mentionnées au I de l'article 8 sont « les données à caractère personnel qui révèlent la prétendue origine raciale ou l'origine ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale d'une personne physique ou de traiter des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique » dites données «sensibles».

20 **En l'espèce**, le décret attaqué est pris pour l'application de l'article L33-14 du code des postes et des communications électroniques ("CPCE") qui prévoit que :

> « Pour les besoins de la sécurité et de la défense des systèmes d'information, les opérateurs de communications électroniques peuvent recourir, sur les réseaux de communications électroniques qu'ils exploitent, après en avoir informé l'autorité nationale de sécurité des systèmes d'information, à des dispositifs mettant en œuvre des marqueurs techniques aux seules fins de détecter des événements susceptibles d'affecter la sécurité des systèmes d'information de leurs abonnés. »

21 Ce dispositif implique le traitement des communications des abonnés passant par le réseau sur lequel sont mis en œuvre des marqueurs techniques, et donc un traitement de données à caractère personnel pouvant contenir des données sensibles au sens du I de l'article 8.

22 Or, si le gouvernement a publié une étude d'impact le 6 février 2018, celle-ci ne contient aucun passage concernant ce traitement de données à caractère personnel. Aucun document complémentaire n'ayant été publié, une étude d'impact au sens de l'article 70-4 de la loi du 6 février 1978 doit donc être réputée comme inexistante.

23 **En outre, en droit**, l'article 70-4 dispose que :

> « Si le traitement est mis en œuvre pour le compte de l'État, cette analyse d'impact est adressée à la Commission nationale de l'informatique et des libertés avec la demande d'avis prévue à l'article 30.»

24 **En l'espèce**, le traitement est mis en œuvre pour les besoins de la sécurité et de la défense des systèmes d'information, c'est à dire pour le compte de l'État.

25 Aucune étude d'impact n'ayant été réalisée, elle n'a pu être transmise à la la Commission nationale de l'informatique et des libertés qui, par conséquent n'a pas publié d'avis à propos dudit traitement.

26 **En conclusion**, le décret a été adopté en contradiction des dispositions contraignantes précitées et devra donc être annulé.

4 Sur la légalité interne

27 L'essentiel des moyens de légalité interne soulevés par les requérantes repose sur l'incompatibilité des dispositions légales en application desquelles il a été adopté avec la Constitution et le droit européen. Il sera également démontré que le décret attaqué méconnait, par lui-même, tant le droit de l'Union européenne que la Convention européenne de sauvegarde des droits de l'Homme et des libertés fondamentales.

4.1 En ce qui concerne l'absence d'intelligibilité et de prévisibilité de la loi

28 L'article L. 33-14 du CPCE introduit par la loi de programmation militaire prévoit de s'appliquer à deux situations factuelles sensiblement différentes, en échouant à distinguer clairement deux régimes juridiques.

29 Dans la première situation, visée par le premier paragraphe de l'article L 33-14, le dispositif de mise en œuvre de marqueurs techniques est prévu « *aux seules fins de détecter des événements susceptibles d'affecter la sécurité des systèmes d'information de leurs abonnés* », c'est-à-dire pour **protéger les abonnés des opérateurs contre une éventuelle attaque informatique** .

30 Dans la seconde situation, visée au paragraphe suivant, le dispositif est prévu « *aux fins de prévenir la menace, à leur exploitation, en recourant, le cas échéant, à des marqueurs techniques que cette autorité leur fournit* », c'est-à-dire pour **surveiller des systèmes informatiques dont l'ANSSI suppose qu'ils sont impliqués dans des attaques informatiques** , entre autres contre les systèmes informatiques des opérateurs d'importance vitale.

31 Le dispositif technique qui doit être appliqué sera le même dans les deux situations. Celui-ci consiste en une interception de l'ensemble des communications électroniques afin de les soumettre à une analyse permettant d'identifier si tout ou partie de ces communications correspondent à des motifs (des « marqueurs techniques ») identifiés comme étant ceux d'une attaque. Pourtant, les deux situations répondent à des régimes juridiques distincts.

32 En effet, en premier lieu, les communications électroniques qui font l'objet d'une analyse en profondeur contiennent, entre autre, des correspondances privées qui sont soumises au secret. Ces communications électroniques sont également, sans que ce soit contestable, des données à caractère personnel. Dès lors, si le dispositif est destiné à protéger un utilisateur final, tel que cela est prévu par le premier paragraphe de l'article L. 34-14, il est nécessaire que cette interception s'opère sous son contrôle. Une telle interception et analyse ne pourrait donc être autorisée si elle est faite à l'insu de l'utilisateur final et s'il ne dispose pas de moyen effectif de s'y opposer.

33 Or, en l'espèce, l'article R. 9-12-1 du CPCE créé par l'article 2 du décret attaqué prévoit que l'opérateur qui met en œuvre le dispositif de marqueurs technique est tenu de prévenir l'ANSSI, mais s'abstient de prévoir toute forme d'information auprès de l'utilisateur final, dont les communications se retrouvent surveillées et analysées sans

qu'il en soit informé, et sans qu'il ait pu s'y opposer.

34 En second lieu, si le dispositif est destiné à surveiller un système informatique dont le comportement est suspect, comme cela est prévu au deuxième paragraphe de l'article L. 34-14 du CPCE, il est logique que le régime juridique soit distinct de la protection accordée à la personne protégée. Ainsi, la directive dite « Police » (directive 2016/680) prévoit que ce n'est qu'une fois que la suspicion est levée que la personne qui a fait l'objet d'une surveillance (en l'espèce dont le système informatique a fait l'objet d'une surveillance) doit être informée, pour pouvoir exercer ses droits de recours.

35 En effet, il serait illogique d'appliquer l'ensemble des règles aux deux situations puisque la personne surveillée serait prévenue au début et à la fin de cette surveillance, y compris si elle est suspecte.

36 La disposition attaquée, **en ne prévoyant pas de dispositif distinct alors que les deux situations envisagées correspondent à deux situations juridiques différentes**, échoue à atteindre l'objectif, à valeur constitutionnelle, d'intelligibilité et de prévisibilité.

4.2 En ce qui concerne le droit des personnes protégées

37 Dans le cas où le dispositif vise à protéger l'utilisateur final contre une attaque informatique, il convient de préciser, comme énoncé ci-dessus, que les données traitées dans le cadre de ce dispositif concernent notamment des correspondances privées.

38 **En droit**, il est ainsi énoncé dans la directive 2002/58 que « *Les données relatives aux abonnés qui sont traitées dans des réseaux de communications électroniques pour établir des connexions et transmettre des informations* ***contiennent des informations sur la vie privée des personnes physiques et touchent au droit au secret de leur correspondance ainsi qu'aux intérêts légitimes des personnes morales*** » (Considérant 26).

39 Il en résulte que, de manière générale « *les fournisseurs de services tiennent toujours leurs abonnés* ***informés des types de données qu'ils traitent, des finalités de ces traitements et de leur durée*** »(Considérant 26).

40 Concernant les aspects de la protection des droits et libertés fondamentaux n'entrant pas expressément dans le cadre de la directive n°2002/58, il convient d'appliquer les dispositions du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (le « RGPD »).

41 Or, il résulte de la même façon des dispositions du RGPD que la personne concernée par un traitement de données à caractère personnel doit être informé de ce traitement et doit pouvoir s'y opposer.

42 Ainsi, l'article 5 du RGPD énonce que « *les données à caractère personnel doivent être (...) traitées de manière licite, loyale et transparente au regard de la personne concernée (licéité, loyauté, transparence)* ».

43 À ce titre, le Considérant 60 précise que :« *Le principe de traitement loyal et transparent exige que* ***la personne concernée soit informée de l'existence de l'opération de traitement et de ses finalités.*** *Le responsable du traitement devrait fournir*

à la personne concernée toute autre information nécessaire pour garantir un traitement équitable et transparent, compte tenu des circonstances particulières et du contexte dans lesquels les données à caractère personnel sont traitées. En outre, la personne concernée devrait être informée de l'existence d'un profilage et des conséquences de celui-ci ».

44 De la même manière, l'article 21 du RGPD prévoit le droit d'opposition de la personne concernée par un traitement de données à caractère personnel.

45 **En l'espèce**, les personnes concernées ne sont en aucun cas informées du traitement qui est fait de leurs données, ni de la finalité poursuivie par le traitement. Les dispositions attaquées ne prévoient par ailleurs aucun droit d'opposition de la personne concernée. Il en résulte qu'ignorant le traitement, les personnes concernées ne peuvent s'y opposer.

46 **En conclusion**, il en résulte que, dans le cas où la finalité du dispositif est de protéger les utilisateurs finals, les dispositions contestées, tant de la loi que de son décret d'application, ne respectent pas le droit de l'Union et doivent être annulées.

4.3 En ce qui concerne le droit des personnes surveillées

4.3.1 S'agissant du droit applicable

47 **En droit**, l'article 5, §1, de la directive 2002/58 pose l'interdiction de principe « *d'écouter, d'intercepter, de stocker les communications et les données relatives au trafic y afférentes, ou de les soumettre à tout autre moyen d'interception ou de surveillance* » ainsi que d'obtenir « *l'accès à des informations déjà stockées, dans l'équipement terminal d'un abonné ou d'un utilisateur* ».

48 La Cour de justice de l'Union européenne a précisé que « *la protection de la confidentialité des communications électroniques et des données relatives au trafic y afférentes, garantie à l'article 5, §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* » (CJUE, grande chambre, 21 décembre 2016, Tele2 Sverige, Watson et autres, C-2013/15, C-698/15, § 77).

49 L'article 15 de la directive 2002/58 permet aux États membres de prendre certaines mesures dérogeant à cet article 5, notamment pour « *assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales* », mais seulement si ces mesures « *sont prises dans le respect des principes généraux du droit communautaire* ».

50 L'Union européenne a adopté une directive spécifique pour préciser les grands principes à respecter en matière de surveillance policière : la directive 2016/680. Au regard de son article 1er, les dispositions de cette directive s'appliquent à tout traitement de données personnelles réalisé par un État membre « *à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces* ».

51 **En l'espèce**, le décret attaqué se donne comme « objet » de « prévenir et caractériser les menaces pouvant affecter la sécurité des systèmes d'information ». Ces menaces entrent dans la qualification des délits définis aux articles 323-1, 323-2 et 323-3 du code pénal comme :

— « le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé » ;
— « le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé » ;
— « le fait d'introduire frauduleusement des données dans un système de traitement automatisé, d'extraire, de détenir, de reproduire, de transmettre, de supprimer ou de modifier frauduleusement les données qu'il contient ».

52 L'objet du décret attaqué et, par là, de la loi qu'il applique, est ainsi de prévenir et détecter des infractions pénales. Pour poursuivre cet objet, ces dispositions permettent à l'ANSSI de mettre en œuvre des traitements de données personnelles.

53 **En conclusion**, les dispositions contestées doivent au minimum respecter la directive 2016/680.

4.3.2 S'agissant du défaut d'accessibilité et de prévisibilité

54 **En droit**, depuis 1999, de jurisprudence constante, le Conseil constitutionnel considère comme contraires aux articles 4, 5, 6 et 16 de la Déclaration de 1789 les normes dont « *les citoyens ne disposent pas d'une connaissance suffisante* » (Décision no 99-421 DC, 16 décembre 1999, cons. 13). Les actes réglementaires sont tenus de respecter ces mêmes exigences et doivent être suffisamment précis et non équivoques.

55 De plus, la Cour européenne des droits de l'Homme (« CEDH») considère que, pour qu'une ingérence soit « prévue par la loi » au sens de l'article 8§2 de la Convention européenne des droits de l'Homme (« Conv. EDH»), « *la loi doit user de termes assez clairs pour indiquer à tous de manière suffisante en quelles circonstances et sous quelles conditions elle habilite la puissance publique à opérer pareille atteinte secrète, et virtuellement dangereuse, au droit au respect de la vie privée et de la correspondance* » (CEDH, Malone c. Royaume-Uni, 2 août 1984, no 8691/79, §67). La Cour EDH précise ainsi que « *les mots « prévue par la loi », au sens de l'article 8§2, veulent d'abord que la mesure incriminée ait une base en droit interne, mais ils ont trait aussi à la qualité de la loi en cause : ils exigent l'accessibilité de celle-ci à la personne concernée, qui de surcroît doit pouvoir en prévoir les conséquences pour elle* » (CEDH, Kruslin c/ France, 24 avril 1990, no 11801/85, §27).

56 **En l'espèce**, le décret attaqué est inintelligible et manque à cette exigence de clarté et d'accessibilité de la norme.

57 **En premier lieu**, le champ d'application d'un "marqueur technique" n'est pas défini par la loi.

58 La lecture des travaux préparatoires laissent comprendre que cette technique toucherait au contenu des communications électroniques et ne se limiterait pas aux seules données de connexion visées à l'article L. 34-1 du CPCE qui sont soumises à un régime de conservation et d'accès moins protecteur en droit français.

59 À cet égard, Guillaume Poupard, directeur général de l'ANSSI, déclarait lors de son audition à l'Assemblée nationale [1]

« Il va donc de soi que nous traitons des données, y compris des données

1. La retranscription de cette audition est disponible à l'adresse suivante : http ://www.assemblee-nationale.fr/15/cr-cdef/17-18/c1718053.asp

> *personnelles. C'est pourquoi* ***le texte ne loi ne saurait comprendre une disposition visant à rassurer qui interdirait de toucher aux données personnelles : nous y touchons de fait****. L'essentiel est que la finalité reste la détection et que l'on s'en tienne aux données strictement nécessaires et signifiantes. Prenons un exemple :* ***le travail de détection consiste parfois à chercher au fin fond de pièces jointes, dans des courriers électroniques****, pour y détecter un éventuel virus caché. »*

60 Pourtant, l'étendue des données analysées par ces "marqueurs techniques" n'est pas clairement décrite par la loi. Celle-ci ne précise pas que cette mesure induirait une atteinte au contenu des communications électroniques et donc au secret des correspondances. L'imprécision de cette notion engendre un doute dans le régime appliqué et donc dans les garanties et restrictions qui doivent être attachées à une telle technique de surveillance.

61 **En deuxième lieu**, la nature exacte des « marqueurs techniques » n'est pas précisée, ni dans la loi, ni dans le décret attaqué. Ainsi il est impossible de savoir si, comme le cite Guillaume Poupard lors de son audition, les marqueurs porteront sur le contenu de correspondances privées, ou sur l'usage de protocoles informatiques, sur des informations techniques portant sur les communications sans que soit considéré le contenu des communications.

62 **En troisième lieu**, de la même manière, le terme de "menace" est particulièrement imprécis. Ici également, les travaux préparatoires permettent de cerner que les atteintes aux système d'information envisagées sont d'une particulière gravité et d'une faible occurrence – correspondant à une vingtaine de cas chaque année [2].

63 Pourtant, les dispositions contestées n'établissent aucun critère permettant de caractériser une menace justifiant le recours à un telle mesure de surveillance.

64 **En conclusion**, ces imprécisions et le manque de clarté général du dispositif ne permettent pas «d'indiquer de manière suffisante en quelles circonstances et sous quelles conditions elle habilite la puissance publique à opérer pareille atteinte secrète, et virtuellement dangereuse, au droit au respect de la vie privée et de la correspondance», et méconnait ainsi l'article 8§2 de la Convention EDH.

4.3.3 S'agissant de l'ineffectivité du contrôle indépendant

65 **En droit**, l'article 8, §3, de la Charte des droits fondamentaux de l'Union européenne prévoit que « *le respect [des règles sur la protection des données] est soumis au contrôle d'une autorité indépendante* ». La Cour de justice de l'Union européenne en déduit que la mise en œuvre d'une mesure de surveillance par des autorités nationales doit être « *subordonné[e] à un contrôle préalable effectué soit par une juridiction soit par une entité administrative indépendante, et que la décision de cette juridiction ou de cette entité intervienne à la suite d'une demande motivée de ces autorités* » (Tele2, § 120).

66 Ce principe se traduit notamment à l'article l'article 47 de la directive 2016/680, qui prévoit que « *chaque autorité de contrôle dispose de pouvoirs d'enquête effectifs. Ces pouvoirs comprennent au moins celui d'obtenir du responsable du traitement ou du sous-traitant l'accès à toutes les données à caractère personnel qui sont traitées* » et

2. V. l'étude d'impact de la loi en cause, disponible à l'adresse : http ://www.assemblee-nationale.fr/15/pdf/projets/pl0659-ei.pdf

que « *chaque autorité de contrôle dispose de pouvoirs effectifs en matière d'adoption de mesures correctrices* ».

67 **En l'espèce**, les dispositions contestées ont confié le contrôle de la légalité des mesures qu'elles permettent à l'ARCEP. Or, ces dispositions ne confient à l'ARCEP aucun moyen d'accéder « à toutes les données à caractère personnel qui sont traitées » : elle ne réalise son contrôle qu'au regard des informations que lui transmet volontairement l'ANSSI, mais n'a pas le pouvoir d'accéder et d'évaluer matériellement les dispositifs techniques déployés par l'ANSSI sur les systèmes des opérateurs et hébergeurs. Son contrôle ne peut s'opérer que « sur dossier » et jamais « sur pièce » — contrairement à ce que pourrait faire la CNIL en d'autres domaines, pour prendre un exemple notoire.

68 De même, l'ARCEP ne peut prendre aucune mesure correctrice contre une mesure qu'elle aurait identifiée comme étant contraire à la loi. Elle ne peut qu'émettre des recommandations à l'ANSSI, ne disposant par exemple d'aucun pouvoir de sanction.

69 **En conclusion**, le décret attaqué a été pris en application de dispositions légales contraires au droit de l'Union. Il a donc été adopté au prix d'une méconnaissance manifeste du droit de l'Union.

4.3.4 S'agissant du défaut d'information des personnes concernées

70 **En droit**, le premier paragraphe de l'article 13 de la directive 2016/680 exige que, lorsqu'une administration réalise une mesure de surveillance afin de prévenir ou détecter des infractions, celle ci communique aux personnes concernées par ces mesures les informations suivantes : l'identité de l'administration, les finalités de la mesure et les droits de ces personnes. Le deuxième paragraphe du même article exige la communication d'autres types d'informations, telles que la nature des données traitées.

71 Le troisième paragraphe de cet article 13 prévoit que la loi d'un État membre peut autoriser des dérogations aux obligations prévues au deuxième paragraphe, notamment pour « retarder ou limiter la fourniture des informations » qui y sont visées, mais ne permet toutefois aucune dérogation aux obligations d'information prévues au premier paragraphe, que les États doivent donc systématiquement respecter et sans retard possible.

72 De façon plus générale, la Cour de justice de l'Union européenne précise que l'information des personnes concernées quant aux mesures qui les visent ne saurait, en aucun cas, être réalisée au-delà du « *moment où cette communication n'est pas susceptible de compromettre les enquêtes menées* » (Tele2, paragraphe 121).

73 **En l'espèce**, les dispositions contestées ne prévoient aucune information, à aucun moment, des personnes contre lesquelles l'ANSSI déploie des dispositifs de surveillance.

74 **En conclusion**, le décret attaqué a été pris en application de dispositions légales contraires au droit de l'Union. Par suite, il est lui-même contraire au droit de l'Union.

4.3.5 S'agissant du défaut de recours effectif

75 **En droit**, l'article 47 de la Charte des droits fondamentaux de l'Union européenne prévoit que « *toute personne dont les droits et libertés garantis par le droit de l'Union ont*

été violés a droit à un recours effectif devant un tribunal », figurant au titre de ces droits et libertés le droit au respect de la vie privée et à la protection des données personnelles, garantis aux article 7 et 8 de cette Charte.

76 Cette exigence est reprise à l'article 54 de la directive 2016/680, qui exige que « *les États membres prévoient que [...] une personne concernée a droit à un recours juridictionnel effectif lorsqu'elle considère que ses droits prévus dans les dispositions adoptées en vertu de la présente directive ont été violés* ».

77 Dans le même sens, l'article 52 de cette directive exige que « *les États membres prévoient que toute personne concernée a le droit d'introduire une réclamation auprès d'une autorité de contrôle unique, si elle considère que le traitement de données à caractère personnel la concernant constitue une violation des dispositions adoptées en vertu de la présente directive* ».

78 **En l'espèce**, les dispositions contestées n'ouvrent aucune possibilité de recours juridictionnel aux personnes concernées qui, en tout état de cause, ne pourraient l'exercer à défaut d'avoir pu prendre connaissance des mesures mises en œuvre à leur encontre, qu'elles ne peuvent ainsi matériellement contester. De même, les dispositions attaquées ne prévoient aucune possibilité pour les personnes concernées d'introduire une réclamation auprès de l'autorité désignée pour contrôlée la légalité des mesures mises en œuvre, l'ARCEP.

79 Enfin, les dispositions attaquées n'ouvrent aucune voie de recours juridictionnel ou de réclamation devant l'ARCEP aux opérateurs et hébergeurs ayant reçu ordre de l'ANSSI de déployer sur leurs systèmes les dispositifs de cette dernières, et ce alors même que ces opérateurs et hébergeurs, telles que les requérantes, auraient pris auprès de leurs utilisateurs l'engagement que leurs systèmes ne soient pas dévoyés à des fins de surveillance illicite.

80 **En conclusion**, le décret attaqué a été pris en application de dispositions légales contraires au droit de l'Union. Partant, il viole de toute évidence le droit de l'Union.

PAR CES MOTIFS, les requérantes concluent à ce qu'il plaise au Conseil d'État :

1. ANNULER le décret n° 2018-1136 du 13 décembre 2018 pris pour l'application de l'article L. 2321-2-1 du code de la défense et des articles L. 33-14 et L. 36-14 du code des postes et des communications électroniques, avec toutes conséquences de droit ;
2. METTRE A LA CHARGE de l'État le versement de la somme de 1024 € sur le fondement de l'article L. 761-1 du code de justice administrative.

Le 14 février 2019, à Paris

Pour les associations La Quadrature du Net, Franciliens.net et la
Fédération des fournisseurs d'accès associatifs à Internet,
Alexis FITZJEAN O COBHTHAIGH
Avocat au Barreau de Paris