ALEXIS FITZJEAN Ó COBHTHAIGH
Avocat au Barreau de Paris
5, rue Daunou - 75002 PARIS
Tél. 01.53.63.33.10 - Fax 01.45.48.90.09
afoc@afocavocat.eu

CONSEIL D'ÉTAT

SECTION DU CONTENTIEUX

REQUÊTE

POUR : **L'association La Quadrature du Net (LQDN), 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 M. Bastien Le Querrec, membre du collège solidaire en exercice.**

CONTRE : **Le décret no 2020-1511 du 2 décembre 2020 modifiant les dispositions du code de la sécurité intérieure relatives au traitement de données à caractère personnel dénommé « Prévention des atteintes à la sécurité publique »**

L'exposante défère le décret attaqué à la censure du Conseil d'État et en requiert l'annulation en tous les chefs lui faisant griefs, par la présente requête.

Table des matières

FAITS

1. L'association « La Quadrature du Net » (LQDN), exposante, promeut et défend les libertés fondamentales dans l'environnement numérique.

2. Par un décret n° 2009-1249 du 16 octobre 2009, le ministre de l'intérieur a été autorisé à mettre en œuvre un traitement de données à caractère personnel intitulé « Prévention des atteintes à la sécurité publique » (ci-après intitulé le « fichier PASP »). Il était notamment indiqué que ce traitement avait pour finalité de « *recueillir, de conserver et d'analyser les informations qui concernent des personnes dont l'activité individuelle ou collective indique qu'elles peuvent porter atteinte à la sécurité publique* ».

3. Le décret n° 2013-1113 du 4 décembre 2013 a codifié ces dispositions aux articles R. 236-11 à R. 236-20 du code de la sécurité intérieure.

4. Le décret n° 2020-1511 du 2 décembre 2020 modifie les dispositions du code de la sécurité intérieure relatives au fichier PASP.

5. Ce décret prévoit notamment l'extension du fichier PASP aux personnes physiques ou morales ou aux groupements « *dont l'activité individuelle ou collective indique qu'elles peuvent porter atteinte à la sécurité publique ou à la sûreté de l'Etat* ». Il prévoit aussi le fichage des « *opinions politiques* », des « *convictions philosophiques* » et de plusieurs catégories de données de santé.

6. C'est le décret attaqué.

DISCUSSION

I. Sur l'intérêt à agir de l'exposante

7. D'emblée, il convient de relever que l'association exposante est bien recevable à contester la légalité de l'arrêté attaqué devant le Conseil d'État.

8. Aux termes de l'article 3 de ses statuts (pièce n° 2), LQDN est une association constituée conformément à la loi du 1er juillet 1901 qui a notamment pour objet « *la promotion et la défense des droits et des libertés fondamentales dans l'environnement numérique* », et notamment « *la lutte contre la surveillance généralisée ou politique, d'origine privée ou publique* » et « *la lutte contre l'utilisation d'outils numériques à des fins de surveillance illégitime* ».

9. L'intérêt à agir de La Quadrature du Net a déjà été reconnu à l'encontre du décret n° 2016-1560 du 28 octobre 2016 autorisant la création d'un traitement de données à caractère personnel relatif aux passeports et aux cartes nationales d'identité (*cf.* CE, 18 octobre 2018, *La Quadrature du Net e.a.*, n° 404996). Un « intérêt spécial » lui a également été reconnu par le Conseil constitutionnel, qui a accepté son intervention au soutien de la QPC n° 2019-797 à propos de la création d'un fichier des ressortissants étrangers se déclarant mineurs non accompagnés (*cf.* Cons. const., 26 juillet 2019, *UNICEF e.a.* n° 2019-797 QPC).

10. Or, le décret attaqué, en ce qu'il concerne un traitement de données personnelles, et *a fortiori* un traitement de données sensibles, participe à l'accentuation du fichage sur la population et affecte directement l'exercice des droits fondamentaux dans l'environnement numérique que l'association exposante entend défendre. En particulier, en étendant de manière disproportionnée la liste des personnes concernées par les traitements et les données pouvant être collectées, le décret attaqué viole les règles relatives à la protection des données personnelles et participe à une augmentation du fichage généralisé contre lequel l'association exposante s'est donnée

pour mission de lutter.

11. **En conclusion**, l'objet statutaire de l'association exposante ainsi que les actions, notamment juridictionnelles, qu'elle a entreprise depuis plusieurs années en ce sens caractérisent manifestement son intérêt à agir à l'encontre du décret attaqué et démontre la recevabilité de la présente requête, adressée en outre dans le délai requis.

II. Sur l'illégalité externe de la décision attaquée

12. Le décret attaqué méconnaît le II de l'article 31 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (ci-après la loi « Informatique et Libertés ») et a ainsi été adopté à l'issue d'une procédure irrégulière.

13. **En droit**, le II de l'article 31 de la loi Informatique et Libertés dispose que les « *traitements qui portent sur des données mentionnées au I de l'article 6 sont autorisés par décret en Conseil d'État pris après avis motivé et publié de la commission* ». Le I de l'article 6 mentionne notamment les données qui révèlent « *les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale d'une personne physique* » ainsi que les « *données concernant la santé* ».

14. Lorsqu'un décret doit être pris après avis de la CNIL, le texte retenu par le Premier ministre ne peut être différent du projet qu'il avait soumis à la CNIL que dans la stricte limite des modifications découlant directement des préconisations de la CNIL (*cf. mutatis mutandis* CE, 28 avril 1954, *Commune de Willer-sur-Thur*, Rec. p. 237 ; CE, Ass., 6 mars 1959, *Association générale des administrateurs civils*, Rec. p. 164 CE, 16 octobre 1968, *Union nationale des grandes pharmacies de France*, n^os^ 69186, 69206 et 70749, Rec. p. 488 ; CE, Ass., 1er juin 1973, *Syndicat national du personnel navigant commercial*, Rec. p. 388 ; CE, 2 mai 1990, *Joannides*, n° 86662 ; CE, Ass., 23 octobre 1998, *Union des fédérations CFDT des fonctions publiques et assimilées*, n° 169797 ; CE, 9 décembre 2011, *Ordre des avocats de Strasbourg*, n° 334463, Rec. T. p. 750 ; CE, 25 janvier 2012, *Association nationale des psychologues de la petite enfance e.a.*, n° 342210 ; CE 4 décembre

2013, *Association France Nature Environnement*, n° 357839, Rec. T. p. 398).

15. Autrement dit, « *même si l'autorité administrative n'est pas liée par l'avis, elle ne peut pas adopter un texte traitant de "questions nouvelles" par rapport au projet soumis à consultation et aux observations ou suggestions éventuellement émises par l'organisme (CE, 28 avril 1954, Commune de Willer-sur-Thur, Rec. p. 237)* » (*cf.* Guide de légistique, p. 130, 2017, La documentation française).

16. **En l'espèce**, le 2° de l'article 3 du décret attaqué prévoit que le fichier PASP peut désormais contenir des données relatives à « *des opinions politiques, des convictions philosophiques, religieuses* », là où ce fichier ne pouvait contenir que des données relatives à « *des activités politiques, philosophiques, religieuses* ».

17. Dans un communiqué publié sur son site Web le 11 décembre 2020, la CNIL a expliqué qu'elle « *ne s'est pas prononcée sur cette modification, qui ne figurait pas dans le projet qui lui avait été soumis* » (*cf.* pièce n° 4).

18. **En conclusion**, le 2° de l'article 3 du décret attaqué a été adopté en violation du II de l'article 31 de la loi Informatique et Libertés et doit conséquemment être annulé.

19. Patente, cette irrégularité justifie, à elle seule, la censure.

III. Sur l'illégalité interne de la décision attaquée

A. En ce qui concerne l'absence de finalités déterminées, explicites et légitimes

20. Le décret attaqué méconnaît l'article 4 de la loi Informatique et Libertés dès lors que sa finalité n'est ni déterminée, ni explicite, ni légitime.

21. **En droit**, le 2° de l'article 4 de la loi Informatique et Libertés dispose que les données doivent être collectées selon des « *finalités déterminées, explicites et légitimes* ».

22. Plus particulièrement, en matière de surveillance, la Cour de justice de l'Union européenne a rappelé, en se fondant notamment sur la Charte des droits fondamentaux de l'Union européenne, que « *pour satisfaire à l'exigence de proportionnalité, une réglementation doit prévoir des règles claires et précises régissant la portée et l'application de la mesure en cause et imposant des exigences minimales, de telle sorte que les personnes dont les données à caractère personnel sont concernées disposent de garanties suffisantes permettant de protéger efficacement ces données contre les risques d'abus.* [...] *Ces considérations valent en particulier lorsqu'est en jeu la protection de cette catégorie particulière de données à caractère personnel que sont les données sensibles* » (*cf.* CJUE, grd. ch., 6 octobre 2020, *La Quadrature du Net e. a.*, n^os^ C-511/18 et C-512/18, pt. 132)

23. La Cour a précisé que les mesures de surveillance réalisées par les États membres doivent « *répondre à des critères objectifs, établissant un rapport entre les données à conserver et l'objectif poursuivi* » et « *s'avérer, en pratique, de nature à délimiter effectivement l'ampleur de la mesure et, par suite, le public concerné* » (*cf.* arrêt *La Quadrature du Net*, préc., pt. 133 ; CJUE, grd. ch. 21 décembre 2016, *Tele2*, n^o^ C-203/15, pt. 110).

24. De même, pour la Cour européenne des droits de l'Homme, « *le pouvoir de surveiller en secret les citoyens n'est tolérable d'après la Convention que dans la mesure strictement nécessaire à la sauvegarde des institutions démocratiques* » (*cf.* Cour EDH, 6 septembre 1978, *Klass e.a. c/ Allemagne*, n^o^ 5029/71, §. 42).

25. Plus précisément, la Cour européenne des droits de l'Homme souligne que « *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* », car la loi « *irait à l'encontre de la prééminence du droit si le pouvoir d'appréciation accordé à l'exécutif ne connaissait pas de limites* » (*cf.* Cour EDH, 2 août 1984, *Malone c/ Royaume-Uni*, n^o^ 8691/79 ; Cour EDH, 29 juin 2006, *Weber et Saravia c/ Allemagne*, n^o^ 54934/00, §. 95).

26. **En l'espèce**, l'article 1^er^ du décret attaqué modifie l'article R. 236-11 du code de la sécurité intérieure afin d'ajouter une nouvelle finalité permettant le recueil, la conservation et l'analyse des informations concernant des personnes physiques ou morales ainsi que des groupements dont l'activité individuelle ou collective indique qu'elles peuvent porter atteinte « *à la sûreté de l'Etat* ». Cette notion est

définie par le même article comme « *des activités susceptibles de porter atteinte aux intérêts fondamentaux de la Nation ou de constituer une menace terroriste portant atteinte à ces mêmes intérêts* ».

27. En l'absence de définition au sein du décret, la notion d'« *intérêts fondamentaux de la Nation* » doit s'apprécier au regard des dispositions existantes dans le code de la sécurité intérieure afin de déterminer le champ d'application de la nouvelle finalité désormais poursuivie par le fichier PASP.

28. **En premier lieu**, l'article L. 811-3 du code de la sécurité intérieure prévoit expressément que la défense et la promotion des intérêts fondamentaux de la Nation peuvent recouvrir les finalités suivantes :

— « *l'exécution des engagements européens et internationaux de la France* » (2° de l'article L. 811-3 du code de la sécurité intérieure), ce qui inclut notamment l'application des normes de l'Union européenne sur l'agriculture, la pêche, les transports, l'emploi, la culture ou le tourisme ainsi que les accords internationaux tels que l'accord de Paris de 2015 sur le climat ou la Convention de Genève de 1931 sur le droit de timbre en matière de chèque ;

— la défense des « *intérêts économiques, industriels et scientifiques de la France* » (3° de l'article L. 811-3 du code de la sécurité intérieure), qui permet l'espionnage industriel et scientifique ;

— les prévention des « *violences collectives de nature à porter gravement atteinte à la paix publique* » (c du 5° de l'article L. 811-3 du code de la sécurité intérieure), couvrant notamment la lutte contre les manifestations, même non-violentes, n'ayant pas été déclarées ou ayant fait l'objet d'une déclaration incomplète (*cf.* Cons. const., 23 juillet 2015, *Loi relative au renseignement*, n° 2015-713 DC, pt. 10 : cette décision renvoie aux articles 431-1 à 431-10 du code pénal pour définir cette finalité, notamment celle prévue à l'article 431-9 du code pénal) ;

— « *la prévention de la criminalité et de la délinquance organisée* » (6° de l'article L. 811-3 du code de la sécurité intérieure), notamment la lutte contre l'acquisition illicite de stupéfiants, même par un individu seul qui n'agit pas en groupe (*cf.* Cons. const., 23 juillet 2015, *Loi relative au renseignement*, n° 2015-713 DC : cette décision renvoie aux infractions listées à l'article 706-73 du code de procédure pénale pour définir cette finalité, notamment celle

prévue à l'article 222-37 du code pénal).

29. Ces finalités, particulièrement nombreuses et larges, sont laissées à la seule discrétion, voire à l'arbitraire, de la police administrative, dès lors qu'elles ne répondent à aucun critère objectif permettant de délimiter effectivement l'ampleur des mesures de surveillance qu'elles justifient. Il en va notamment de la défense des « *intérêts majeurs de la politique étrangère* », de « *l'exécution des engagements européens et internationaux* » ou de la défense des « *intérêts économiques, industriels et scientifiques* » de la France.

30. En effet, il serait déraisonnable de prétendre pouvoir définir les contours concrets de tels intérêts, lesquels conditionnent pourtant une surveillance ainsi définie unilatéralement par le pouvoir exécutif sans prévisibilité pour les personnes susceptibles d'en être affectées.

31. **En second lieu**, la rédaction de l'article 1er du décret attaqué n'autorise pas seulement le traitement de données personnelles des personnes dont les activités portent directement et effectivement atteinte à la sûreté de l'État mais englobe également les données de toute personne dont les activités font entrevoir une simple *potentialité* d'atteinte, ou sont « *susceptibles de porter atteinte* » aux intérêts de la Nation. En pratique, cette disposition permet le traitement de données d'un grand nombre de personnes, pourvu que celles-ci soient seulement sujettes à un simple doute, qu'il appartient aux seuls agents de déterminer.

32. Autrement dit, non seulement le champ des personnes concernées est trop étendu, mais encore est-il insuffisamment défini. Ces lacunes sont d'autant plus inquiétantes et problématiques que la qualification des données n'appartient qu'à l'administration.

33. **En conclusion**, la finalité litigieuse ajoutée au fichier PASP est manifestement indéterminée, équivoque, illégitime et imprévisible, dès lors qu'elle n'est pas encadrée par des critères objectifs précis permettant de limiter efficacement le traitement.

B. En ce qui concerne l'extension du champ des personnes concernées

34. Le décret attaqué méconnaît le 3° de l'article 4 de la loi Informatique et Libertés et l'article 3 de la Convention internationale des droits de l'enfant (CIDE) des Nations-Unies du 20 novembre 1989.

1. S'agissant de l'entourage et des victimes

35. **En droit**, le 3° de l'article 4 de la loi Informatique et Libertés prévoit que « *les données à caractère personnel doivent être* [...] *limitées à ce qui est nécessaire* ». En matière de surveillance, ce principe de limitation s'applique notamment aux personnes surveillées. Ainsi, une mesure de surveillance est contraire à la Constitution si elle « *s'applique également aux personnes appartenant à l'entourage de la personne concernée par l'autorisation, dont il existe des raisons sérieuses de penser qu'elles sont susceptibles de fournir des informations au titre de la finalité qui motive l'autorisation* » dès lors que cette mesure permet qu'un nombre élevé de personnes fasse l'objet de cette technique de renseignement, sans que leur lien avec la menace soit nécessairement étroit (*cf.* Cons. constit., 4 août 2017, n° 2017-648 QPC, pt. 11).

36. **En l'espèce**, l'article 2 du décret attaqué crée un article R. 263-12 qui, à ses II, III et IV, prévoit que peuvent désormais être fichées les personnes « *entretenant ou ayant entretenu des relations directes et non fortuites avec la personne pouvant porter atteinte à la sécurité publique ou la sûreté de l'Etat* », ainsi que « *les victimes des agissements de* [cette dernière] ».

37. **En premier lieu**, ce fichage est particulièrement large et intrusif. Il est ainsi notamment susceptible de couvrir l'essentiel des catégories de données listées au I de l'article R. 263-12 du code de la sécurité intérieure telles que les photographies, les lieux fréquentés, les activités sur les réseaux sociaux ou les activités religieuses, sans que l'importance de cette diversité ne soit justifiée par aucun élément objectif.

38. En pratique, un rapport de 2018 du référent PASP décrit une façon particulièrement massive et généralisée dont ces données peuvent être exploitées : « *L'ac-*

cès à l'application PASP se fait par le portail sécurisé "CHEOPS" qui [...] *dispose d'une fonctionnalité originale, en cours d'enrichissement par des développements complémentaires. Il s'agit d'une gestion de liens pertinents entre individus du fichier qui aboutit à élaborer graphiquement des sociogrammes (leader d'un groupe, membres du groupe, antagonistes...)* » (*cf.* pièce n° 5. pt. I. 1. 4., p. 11).

39. **En deuxième lieu**, la notion de « *relation directe et non fortuites* », lorsqu'elle s'applique à des relations avec les « *groupements* » visés à l'article R. 236-11 du code de la sécurité intérieure, permet de ficher l'ensemble des participants à une manifestation, peu importe que ces participants soient ou non considérés comme représentant une menace. Ainsi, le rapport de 2018 du référent PASP indiquait déjà que « *certaines notes se bornent à faire état de faits collectifs, notamment pour les phénomènes de bande ou les manifestations, avec une tendance à inclure dans le traitement toutes les personnes contrôlées ou interpelées alors qu'il n'est fait état dans la note d'aucun fait personnel qui leur est reproché* » (*cf.* pièce n° 5, précitée, pt. III. 3. 3., p. 23). Cette pratique, balbutiante en 2018, pourra être amplifiée et généralisée par le décret attaqué.

40. **En troisième lieu**, la notion de « *victimes des agissements pouvant porter atteinte à la sécurité publique ou la sûreté de l'Etat* » est laissée à l'interprétation arbitraire des agents dans la mesure où cette notion est dépourvue de signification juridique, ne renvoyant à aucune infraction ou procédure pénale.

41. **En conclusion**, le décret attaqué permet d'enregistrer des données particulièrement intrusives concernant un « nombre élevé de personnes, sans que leur lien avec la menace soit nécessairement étroit » mais, au contraire, laissé à l'arbitraire des agents, augmentant considérablement le risque que ceux-ci abusent de leurs pouvoirs, en violation du 3° de l'article 4 de la loi Informatique et Libertés.

2. S'agissant des mineurs

42. **En droit**, l'article 3 §. 1er de la Convention des Nations-Unies du 20 novembre 1989 relative aux droits de l'enfant prévoit que, « *dans toutes les décisions qui concernent les enfants, qu'elles soient le fait des institutions publiques ou privées de protection sociale, des tribunaux, des autorités administratives ou*

des organes législatifs, l'intérêt supérieur de l'enfant doit être une considération primordiale ».

43. Ces stipulations sont directement applicables en droit interne (*cf.* not. CE, 22 septembre 1997, *Cinar*, n° 161364, Rec. p. 319 ; CE, 6 novembre 2000, *GISTI*, n° 204784, Rec. T. p. 1031).

44. Par ailleurs, par deux décisions du 21 mars 2019, le Conseil constitutionnel a explicitement consacré la protection de l'intérêt supérieur de l'enfant en la rattachant aux dixième et onzième alinéas du Préambule de la Constitution de 1946 (*cf.* Cons. const., 21 mars 2019, *M. Adama Soumaoro [Examens radiologiques osseux aux fins de détermination de l'âge]*, n° 2018-768 QPC, pt. 6 ; Cons. const. 21 mars 2019, *Loi de programmation 2018-2022 et de réforme pour la justice* , n° 2019-778 DC, pt. 60).

45. En matière de surveillance policière, ce principe est notamment traduit au considérant 50 de la directive n° 2016/680 du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes 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, et à la libre circulation de ces données (ci-après directive « police-justice »), qui précise que « *les mesures prises par le responsable du traitement devraient comprendre l'établissement et la mise en œuvre de garanties spécifiques destinées au traitement de données à caractère personnel relatives aux personnes physiques vulnérables telles que les enfants* ».

46. **En l'espèce**, jusqu'à l'édiction du décret attaqué, les personnes pouvant être fichées étaient limitées à celles âgées « *d'au moins treize ans* » et « *dont l'activité individuelle ou collective indique qu'elles peuvent porter atteinte à la sécurité publique* » (article R. 236-15 du code de la sécurité intérieure).

47. Désormais, depuis l'entrée en vigueur du décret attaqué, peuvent aussi être fichées les personnes qui font partie de l'entourage des personnes représentant une menace, ainsi que leurs victimes (article R. 263-12, II, III et IV, tel que créé par l'article 2 du décret attaqué). Or, le fichage de ces nouvelles personnes n'est accompagné d'aucune garantie quant à leur âge. En effet, l'article 5 du décret attaqué

précise explicitement que la limite d'âge prévue par l'article R. 236-15 ne s'applique qu'aux personnes « *pouvant porter atteinte à la sécurité publique ou à la sûreté de l'Etat* ».

48. **En conclusion**, l'article 2 du décret attaqué autorise à enregistrer des données particulièrement intimes sur des enfants de tout âge sans prévoir aucune garantie spécifique pour protéger l'intérêt supérieur de ceux-ci, et doit être annulé de ce seul fait.

C. En ce qui concerne l'extension des catégories de données traitées

49. Le décret attaqué méconnaît les articles 4 et 88 de la loi Informatique et Libertés, en ce que les données personnelles dont il autorise le traitement sont inadéquates, non pertinentes au regard des finalités pour lesquelles elles sont traitées et non limitées à ce qui est absolument nécessaire.

50. **En droit**, l'article 4 de la loi Informatique et Libertés prévoit que les données personnelles doivent être « *adéquates, pertinentes et, au regard des finalités pour lesquelles elles sont traitées, limitées à ce qui est nécessaire* ». Il est précisé que pour les données relevant du titre III, c'est-à-dire les données relevant de la directive « police-justice », celles-ci ne doivent pas être excessives.

51. Par ailleurs, dans le cadre des traitements relevant de la directive « police-justice », l'article 88 de la loi Informatique et Libertés précise que le traitement sur les « *opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale d'une personne physique ou* [les] *données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique* » n'est « *possible uniquement en cas de nécessité absolue, sous réserve de garanties appropriées pour les droits et libertés de la personne concernée* ». Autrement dit, ces données ne peuvent être traitées que s'il est impossible d'atteindre l'objectif poursuivi sans les traiter.

52. Enfin, dans le cadre d'un recours formé contre la précédente version du fichier PASP, le Conseil d'État avait autorisé le traitement des données relatives à des « *activités politiques, philosophiques, religieuses ou syndicales* » à la condition

que ces données soient « *de nature factuelle et objective* » (*cf.* CE, 11 mars 2013, *Association SOS Racisme*, n° 332886).

53. **En l'espèce**, le décret attaqué prévoit l'extension du traitement des données aux opinions politiques, convictions philosophiques, religieuses ou relatifs une appartenance syndicale (1), à plusieurs types de données de santé (2) ainsi qu'aux activités en ligne (3).

1. S'agissant des opinions politiques et convictions religieuses

54. Le décret attaqué prévoit la possibilité de collecte, de conservation et de traitement de données relatives à « *des opinions politiques, des convictions philosophiques, religieuses ou une appartenance syndicale* ».

55. **En premier lieu**, un tel traitement de données avait déjà auparavant été autorisé dans le cadre du fichier dit « EDVIGE » créé par le décret n° 2008-632. Or, à la suite d'une forte mobilisation contre l'étendue des données concernées par ce traitement « EDIVGE », ce décret avait été retiré par le décret n° 2008-1199 du 19 novembre 2008.

56. **En second lieu**, le traitement de telles données n'est en aucun adéquat, pertinent ou limité à ce qui est nécessaire. Il est par là même évident qu'aucune « *nécessité absolue* », au sens de la directive « police-justice », n'est susceptible, au cas présent, de venir légalement justifier le traitement de telles données.

57. Au contraire, il est impossible de comprendre l'intérêt que pourrait avoir l'enregistrement de données relatives aux opinions, convictions religieuses ou appartenances syndicales avec la finalité poursuivie, c'est-à-dire la prévention des atteintes à la « *sécurité publique* » ou à la « *sûreté de l'Etat* ».

58. Il n'est pas plus justifié en quoi le traitement de ces données serait subitement devenu absolument nécessaire à la finalité poursuivie.

59. Le traitement de telles données ne peut pas, par ailleurs, respecter les conditions établies auparavant par le Conseil d'État sur la précédente version du fichier

PASP pour lequel seules des données factuelles et objectives pouvaient être traitées.

2. S'agissant des données de santé

60. Le décret attaqué autorise le traitement de « *données de santé révélant une dangerosité particulière* » (article 3) ainsi que les « *données relatives aux troubles psychologiques ou psychiatriques* », aux « *comportements auto-agressifs* » et aux « *addictions* » (article 2).

61. De la même manière que pour les données relatives aux opinions politiques, convictions religieuses ou appartenances syndicales, aucune justification n'est avancée par le ministère de l'intérieur quant à la pertinence, l'adéquation ou la nécessité du traitement de telles données.

62. À ce titre, il est particulièrement difficile de comprendre en quoi le traitement de données relatives à des troubles psychologiques ou psychiatriques ou à des comportements auto-agressifs serait nécessaire et même « *absolument nécessaire* », au sens de la directive « police-justice », à la prévention de la sécurité publique ou la sûreté de l'État.

63. Par ailleurs, de telles qualifications ne relèveront non pas de professionnels de l'ordre médical mais simplement des services de police concernés. Ces derniers se retrouveront donc seuls à même de déterminer les troubles psychologiques ou psychiatriques d'un individu. Il est évident qu'une telle qualification va encore une fois à l'encontre de la jurisprudence du Conseil d'État (*cf.* CE, 11 mars 2013, n° 332886, préc.) selon laquelle seules des « *données factuelles ou objectives* » peuvent être traitées dans le fichier PASP.

3. S'agissant des données relatives aux activités en ligne

64. Le décret attaqué prévoit d'autoriser le traitement des données relatives aux « *activités sur les réseaux sociaux* ».

65. **En premier lieu**, le traitement de données relatif à une notion aussi large et peu précise que celles des « *activités sur les réseaux sociaux* » est incompatible avec les exigences de la loi Informatique et Libertés sur des traitements adéquats, pertinents et non-excessifs.

66. Il faut à ce titre souligner que la notion de « *réseaux sociaux* » n'étant pas définie, elle peut concerner de multiples plateformes et sites Web (forums, espaces de commentaires sur un site, plateformes d'achat et de vente de biens, . . .). La notion d'« *activités* » peut elle aussi recouvrir de nombreuses pratiques, allant de la simple consultation d'un site, à la saisie de textes en passant par le fait de poster des vidéos ou des photos.

67. En particulier, le ministre de l'intérieur n'a pas voulu se cantonner aux sites internet des opérateurs de plateforme en ligne mentionnés au 2° du I de l'article L. 111-7 du code de la consommation, définition habituellement donnée des « réseaux sociaux », notamment à l'article 154 de la loi n° 2019-1479 du 28 décembre 2019 de finances pour 2020. Cette absence de bornage textuel ne peut traduire qu'une volonté de ne pas borner l'ampleur de la surveillance sur Internet et, ce faisant, permettre un traitement disproportionné de données personnelles.

68. Autrement dit, une telle notion permettrait de traiter n'importe quelle donnée personnelle issue de l'activité en ligne d'une personne, hors toute notion de nécessité, d'adéquation ou de proportionnalité.

69. C'est d'ailleurs également l'avis de la CNIL dans sa délibération n° 2020-064 du 25 juin 2020 qui a considéré que « *les dispositions du projet de décret ne permettent pas une compréhension claire et précise de la nature des données susceptibles d'être enregistrées à ce titre, ni des modalités de cette collecte, pouvant par exemple renvoyer à des réalités différentes selon la politique de confidentialité du réseau concerné* ».

70. **En second lieu**, le décret attaqué ne permet pas d'éviter une collecte automatisée des données, allant ce faisant à l'encontre des principes de nécessité, d'adéquation ou de proportionnalité.

71. Cette absence de précision a été relevée par la CNIL dans sa délibération

n° 2020-064, qui demande « *qu'il* [soit] *également* [exclu] *explicitement la possibilité d'une collecte automatisée de ces données* ».

72. Par ailleurs, la CNIL avait déjà relevé, dans sa délibération 2019-114 du 12 septembre 2019 portant avis sur le projet d'article 9 du projet de loi de finances pour 2020 (dispositif d'analyse et de collecte automatisée de données publiées sur Internet), qu'un tel dispositif serait notamment de nature à « *modifier, de manière significative, le comportement des internautes qui pourraient alors ne plus être en mesure de s'exprimer librement sur les réseaux et plateformes visés et, par voie de conséquence, de rétroagir sur l'exercice de leur libertés* » (CNIL, 12 septembre 2019, délibération n° 2019-114).

73. Or, en n'interdisant pas la collecte automatisée de données sur Internet, combiné à l'absence de définition précise de la notion d'« *activités sur les réseaux sociaux* », le décret attaqué permet de collecter un nombre virtuellement infini de données personnelles, sans qu'aucune limite, ni explicite, ni implicite, ne vienne encadrer cette collecte.

74. Ainsi, en autorisant la collecte des informations relatives aux « *activités sur les réseaux sociaux* », le décret attaqué autorise un traitement qui n'est ni nécessaire, ni adéquat, ni proportionné au but poursuivi.

75. **En conclusion**, le décret attaqué méconnaît les article 4 et 88 de la loi Informatique et Libertés.

D. En ce qui concerne l'intensification de l'exploitation des données

1. S'agissant des rapprochements entre fichiers

76. Le décret attaqué méconnaît l'article 92 de la loi Informatique et Libertés, dès lors qu'il instaure des opérations de rapprochements dont la nécessité et la proportionnalité à l'objectif poursuivi font défaut et ne sont garantis par aucune limite, notamment concernant la liste des fichiers pouvant être recoupés avec le PASP.

77. **En droit**, l'article 92 de la loi Informatique et Libertés prévoit que les traitements mis en œuvre pour la poursuite et la prévention des infractions et des atteintes à la sécurité publique « *sont autorisés s'ils sont nécessaires et proportionnés à cette finalité* ». Deux types de traitements méritent un examen particulier. La CNIL les définit ainsi : « *interconnexion (mise en relation automatisée de traitements) ou rapprochement (mise en relation non automatisée de traitements)* » (*cf.* CNIL, délibération n° 2010-456).

78. L'interconnexion et le rapprochement causent des risques de dévoiement d'une ampleur toute singulière et doivent, à ce titre, démontrer répondre à une nécessité et être proportionnels à la hauteur des risques en cause. Ainsi, dans son avis du 11 juin 2009 sur la création du traitement PASP, la CNIL se réjouissait du fait que, suite au retrait du fichier EDVIGE qu'elle avait combattu, « *elle avait également obtenu que le traitement ne fasse l'objet d'aucune interconnexion, aucun rapprochement ni aucune forme de mise en relation avec d'autres fichiers, notamment ceux de police judiciaire* » (CNIL, délibération n° 2009-355 du 11 juin 2009). De même, le Conseil constitutionnel n'hésite pas à considérer l'absence d'interconnexion comme une garantie déterminante afin qu'un fichier de police soit « *de nature à assurer, entre le respect de la vie privée et la sauvegarde de l'ordre public, une conciliation qui n'est pas manifestement déséquilibrée* » (Cons. const., 2 mars 2004, *Loi portant adaptation de la justice aux évolutions de la criminalité*, n° 2004-492 DC, cons. 86).

79. **En l'espèce**, l'article 7 du décret attaqué mentionne explicitement que des opérations manuelles de « *rapprochement* » pourront être réalisées avec le PASP et d'autres fichiers. Dans son avis du 25 juin 2020, la CNIL explique que les entrées du PASP pourront être « *alimentées manuellement* » à partir des informations contenues dans quinze autres fichiers : GIPASP, FSPRT, TAJ, SIS II, FPR, FOVeS, AGRIPPA, AGDREF, API-PNR, SNPC, SIV, GEDRET, FINIADA, EASP et STITCH (CNIL, délibération n° 2020-064 du 25 juin 2020).

80. Dans ce même avis, la CNIL émet de vives critiques : « *il aurait été hautement souhaitable de modifier les actes réglementaires encadrant les fichiers concernés afin de mentionner explicitement qu'ils peuvent faire l'objet d'un rapprochement avec le traitement PASP* ». De même, elle regrette que le décret échoue à « *mentionner explicitement les fichiers effectivement consultés permettant d'alimenter ces catégories* ». En effet, la liste des quinze traitements à partir desquels le

fichiers PASP est alimenté n'a été donnée à la CNIL qu'à titre informatif et n'apparaît pas dans le décret attaqué, de sorte que le gouvernement peut allonger cette liste à l'envie, sans aucune limitation textuelle.

81. **En conséquence**, le décret attaqué instaure des opérations de rapprochements dont la nécessité et la proportionnalité à l'objectif poursuivi font défaut et ne sont garantis par aucune limite, notamment concernant la liste des fichiers pouvant être recoupés avec le PASP, en violation de l'article 92 de la loi Informatique et Libertés.

2. S'agissant des interconnexions entre fichiers

82. Le décret attaqué méconnaît l'article 101 de la loi Informatique et Libertés en ce qu'il instaure des opérations d'interconnexion, sans prévoir un enregistrement de ces dernières dans le journal des opérations.

83. **En droit,** l'article 101 de la loi Informatique et Libertés exige que le responsable d'un fichier de police tienne « *un journal des opérations* » réalisées sur le fichier, notamment des opérations « *d'interconnexion* ». L'acte réglementaire qui autorise le traitement doit donc décrire ces opérations d'interconnexion, ne serait-ce que pour mettre en place le journal des opérations. En dernier ressort, la CNIL peut qualifier ou requalifier une opération que l'acte aurait échoué à qualifier d'interconnexion. Ainsi, par exemple, dans son avis du 9 décembre 2010 sur la création du fichier GIPASP, la CNIL a considéré que, contrairement à ce que le décret prétendait, l'« *interrogation du traitement GIPASP depuis le traitement GSI ne permettra d'accéder qu'à l'information "connu" ou "inconnu". Ainsi,* [...] *la mise en relation automatisée de ces traitements est susceptible d'être qualifiée d'"interconnexion"* ».

84. **En l'espèce**, l'article 2 du décret prévoit que le fichier PASP peut indiquer si une personne est enregistrée ou non dans six autres fichiers prévoyant des traitements (GIPASP, FSPRT, TAJ, SIS II, FPR et FOVeS).

85. Cette information est en soi une opération qui, à lire le décret attaqué et l'avis de la CNIL, est automatisée entre le PASP et les six autres fichiers. Si une personne fichée dans le PASP l'est aussi dans un autre fichier, sa fiche l'indiquera

automatiquement. Le rapport de 2018 du référent PASP, précité, permet de bien saisir le contexte général dans lequel cette interconnexion s'opère : « *l'accès à l'application PASP se fait par le portail sécurisé "CHEOPS" qui permet de donner accès, sous une même configuration, à différentes applications de la police nationale, à des applications réglementaires telles que le fichier national des automobiles ou celui des permis de conduire ou encore à des applications gérées par le ministère de la Justice (fichier des auteurs d'infraction sexuelles, par ex.)* » (*cf.* pièce n° 5 précitée, par. I.1.4., p. 11).

86. Exactement comme pour le GSI qui indiquait qu'une personne était fichée au GIPASP dans l'avis précité de la CNIL en 2010, le PASP doit être considéré comme réalisant des opérations d'interconnexion avec les six fichiers pour lesquels il est prévu d'afficher l'inscription ou non de la personne en question.

87. **En conséquence**, en instaurant, à son article 2, des opérations d'interconnexion, sans prévoir un enregistrement de ces dernières dans le journal des opérations, le décret attaqué viole l'article 101 de la loi Informatique et Libertés.

3. S'agissant des recoupements avec le fichier TES

88. Le décret attaqué méconnaît manifestement l'article 92 de la loi Informatique et Libertés, dès lors qu'il ne prévoit aucun encadrement suffisant de la poursuite de la finalité de prévention des atteintes aux intérêts fondamentaux de la Nation et instaure des opérations d'interconnexions et de rapprochements, notamment avec le fichier TES et le fichier TAJ, sans aucune garantie.

89. **En droit**, l'article 4 du décret n° 2016-1460 du 28 octobre 2016 autorisant la création d'un traitement de données à caractère personnel relatif aux passeports et aux cartes nationales d'identité, dit fichier « TES », autorise les agents de la police nationale et de la gendarmerie nationale à accéder aux données enregistrées dans le fichier TES pour les besoins de la « *prévention des atteintes aux intérêts fondamentaux de la Nation et des actes de terrorisme* ».

90. **En l'espèce**, l'article 1er du décret attaqué permet la collecte de données pour lutter contre les atteintes aux « *intérêts fondamentaux de la Nation* ». Cette

nouvelle finalité est donc identique au motif autorisant l'accès au fichier TES. En l'absence de limitation expresse de cette finalité, rien n'interdit que, dans le cadre d'une mission de prévention des atteintes aux intérêts fondamentaux de la Nation, ces agents puissent simultanément consulter le fichier TES, qui concentre les photographies de la totalité des ressortissants français disposant d'un titre d'identité, et le fichier PASP, afin par exemple de verser ces photographies dans le fichier PASP ou, partant de là, vers d'autres fichiers avec lequel le PASP est interconnecté, tel que le fichier TAJ qui autorise la reconnaissance faciale.

91. L'absence de délimitation précise de la notion d'intérêts fondamentaux de la Nation, couplée à l'absence de délimitation des opérations d'interconnexion et de rapprochement instaurées par le décret attaqué, permet en théorie d'immenses mouvements d'informations particulièrement sensibles afin, dans le pire des scénarios, d'alimenter un système général de reconnaissance faciale.

92. **En conclusion**, le décret attaqué, en ne prévoyant pas d'encadrement suffisant de la finalité de prévention des atteintes aux intérêts fondamentaux de la Nation et en instaurant des opérations d'interconnexions et de rapprochements, notamment avec le fichier TES et le fichier TAJ, sans aucune garantie, dépasse toute proportion raisonnable et viole manifestement l'article 92 de la loi Informatique et Libertés.

E. En ce qui concerne l'insuffisance des garanties organisationnelles

1. S'agissant de l'absence de garanties appropriées

93. Le décret attaqué méconnaît l'article 88 de la loi Informatique et Libertés, dès lors qu'il ne prévoit aucune garantie appropriée pour les droits et libertés des personnes concernées.

94. **En droit**, l'article 88 de la loi Informatique et Libertés prévoit que le traitement de données « *sensibles* » n'est possible que sous réserve « *de garanties appropriées pour les droits et libertés de la personne concernée* ».

95. En matière de surveillance, la Cour de justice de l'Union européenne consi-

dère que, « *aux fins de garantir, en pratique, le respect de ces conditions, il est essentiel que la mise en œuvre de la mesure* [...] *soit soumise à un contrôle préalable effectué soit par une juridiction, soit par une entité administrative indépendante, dont la décision est dotée d'un effet contraignant* » (*cf.* CJUE, 6 octobre 2020, *La Quadrature du Net e.a.*, n° C-511/18, §§. 189 et 192 ; CJUE, 21 décembre 2016, *Tele2*, n^os^ C-203/15 et C-698/15 , §. 120).

96. **En l'espèce**, comme rappelé précédemment, le décret attaqué prévoit le traitement de nouvelles catégories de données personnelles, dont plusieurs données dites sensibles : les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ou encore de nombreuses données de santé.

97. Or, la possibilité de traitement de ces nouvelles catégories de données devrait normalement être entourée de nouvelles garanties spécifiques. Ces garanties sont, au cas présent, inexistantes. Au contraire, en permettant le traitement de catégories de données aussi larges que les opinions politiques ou les convictions religieuses, le décret attaqué délègue à l'autorité chargée du traitement un pouvoir dont il est impossible de garantir un contrôle effectif. L'enregistrement de ces données dépend entièrement de la subjectivité de l'autorité qui l'effectue. Son contrôle est matériellement impossible ce qui annihile totalement l'ensemble des ersatz de garanties qui sont prévues.

98. **En conclusion**, le décret attaqué viole l'article 88 de la loi Informatique et Libertés.

2. S'agissant des larges délais de conservation

99. Le décret attaqué méconnaît le 5° de l'article 4 de la loi Informatique et Libertés, dès lors qu'il prévoit une conservations de données personnes et, notamment, de données sensibles, pendant une durée qui excède de très loin ce qui est nécessaire au regard des finalités pour lesquelles ces données sont traitées.

100. **En droit**, le 5° de l'article 4 de la loi Informatique et Libertés indique que les données personnelles doivent être conservées « *pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées* ».

101. À ce titre, il convient de relever que, dans une décision de 2011, le Conseil constitutionnel a censuré une disposition qui, concernant un traitement de données personnelles effectué à des fins de rassemblement de preuves d'infractions et d'identification de leur auteur, prévoyait l'effacement de certaines données à « *la clôture de l'enquête et, en tout état de cause, à l'expiration d'un délai de trois ans après le dernier acte d'enregistrement* ». Il a en effet considéré que « *la conservation de ces données ne saurait être prolongée à l'initiative de l'enquêteur au-delà de trois ans après leur enregistrement* » (*cf.* Cons. const., 10 mars 2011, *LOPPSI*, n° 2011-625 DC, pt. 72).

102. **En l'espèce**, si le décret attaqué ne modifie pas directement la durée de conservation des données personnelles, il ajoute néanmoins une nouvelle finalité et permet notamment l'enregistrement de plusieurs nouvelles catégories de données personnelles, particulièrement sensibles. Surtout, le décret attaqué étend le fichage à des nouvelles catégories de personnes, entourage et victimes, sans adapter le régime à ces personnes d'aucune façon.

103. Il en résulte que l'ensemble de ces nouvelles données personnelles, ainsi que l'ensemble des données concernant ces nouvelles personnes, seront soumis à la durée de conservation prévue aux articles R. 236-14 et R. 236-15 du code de la sécurité intérieure.

104. Or, ces articles prévoient que les données concernées ne peuvent être conservées plus de dix ans (ou trois ans pour les mineurs) « *après l'intervention du dernier événement de nature à faire apparaître un risque d'atteinte à la sécurité publique ou à la sûreté de l'État ayant donné lieu à un enregistrement* ».

105. Ainsi, de la même manière que pour la disposition censurée par le Conseil constitutionnel en 2011, cette disposition prévoit que la conservation des données est prolongée à l'initiative de l'enquêteur. En effet, chaque fois que celui-ci considère qu'il existe un nouvel évènement lui permettant de modifier le traitement de données existant, le délai de conservation des données est rallongé de trois ou dix ans selon les cas. Cette conservation est alors *de facto* excessive par rapport à la finalité poursuivie.

106. **En conclusion**, en prévoyant le traitement de nouvelles données qui se-

ront soumises à une durée excessive de conservation, le décret attaqué viole le 5° de l'article 4 de la loi Informatique et Libertés.

107. À tous égards, l'annulation du décret attaqué s'impose.

PAR CES MOTIFS, l'association La Quadrature du Net, exposante, conclut qu'il plaise au Conseil d'État de :

ANNULER le décret attaqué, avec toutes conséquences de droit ;

ENJOINDRE au ministre de l'intérieur de supprimer l'ensemble des données collectées en application du décret attaqué, sous astreinte de 1 024 euros par jour de retard, à compter de la notification de la décision à intervenir ;

METTRE À LA CHARGE de l'État une somme de 4 096 euros, en application de l'article L. 761-1 du code de justice administrative.

Fait à Toulouse, le 22 décembre 2020

Alexis FITZJEAN Ó COBHTHAIGH
Avocat au Barreau de Paris

BORDEREAU DES PRODUCTIONS

Pièce n° 1 : Décret attaqué ;

Pièce n° 2 : Statuts de LQDN ;

Pièce n° 3 : Décision du collège solidaire de LQDN du 21 décembre 2020 et pouvoir spécial ;

Pièce n° 4 : Communiqué de la CNIL du 11 décembre 2020, « Publication des décrets relatifs aux fichiers PASP, GIPASP et EASP : la CNIL précise sa mission d'accompagnement » ;

Pièce n° 5 : Rapport public 2017 du référent national, « Traitement de données à caractère personnel : "Prévention des atteintes à la sécurité publique" en ce qu'il concerne les mineurs ».