CONSEIL D'ÉTAT

MÉMOIRE EN RÉPLIQUE
Article L. 521-2 du Code de justice administrative

POUR :

Monsieur Gaspard KOENIG, [redacted]

GENERATIONLIBRE, association régie par la loi du 1er juillet 1901 dont le siège est sis 24, rue Saint-Lazare - 75 009 Paris, prise en la personne de son Président, Monsieur Gaspard KOENIG,

Ayant pour avocats :

Maître Nicolas GARDÈRES
Avocat au Barreau de Paris,
[redacted]

Maître Rubin SFADJ
Avocat au Barreau de Marseille,
[redacted]

CONTRE :

Le 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.

PLAISE AU CONSEIL

Le recours en excès de pouvoir des requérants a entraîné la production en réponse d'observations du ministère de l'Intérieur.

Maintenant l'ensemble de leurs moyens, arguments et demandes, les requérants entendent, pour répondre aux observations du ministère de l'Intérieur, apporter de nouveaux moyens à l'appui de leurs demandes.

Ces nouveaux moyens se rapportent d'une part à la violation par le décret attaqué du principe de proportionnalité (A), et d'autre part à l'entrée en vigueur imminente du nouveau règlement général de l'Union européenne sur la protection des données (B).

A. Sur la violation du principe de proportionnalité

L'objectif du fichier créé par le décret entrepris serait de sécuriser la délivrance des titres et d'améliorer corrélativement la lutte contre la fraude.

S'il n'est pas contesté que cet objectif revêt un caractère d'intérêt général, il demeure indispensable que l'atteinte aux libertés publiques qu'implique nécessairement la création d'un tel fichier présente une utilité réelle relativement à l'objectif qu'il entend remplir.

À cet égard, il convient de rechercher la réalité statistique de la fraude contre laquelle le décret attaqué se propose de lutter. En effet, tous les promoteurs de ce projet partent de l'hypothèse que ladite fraude serait un phénomène endémique et que ce fichier serait une réponse sinon indispensable, du moins nécessaire, à la fraude.

Cependant, les données produites par l'État lui-même démontrent sans ambiguïté que le phénomène fondant la légitimité prétendue du décret attaqué est en réalité minime, pour ne pas dire dérisoire.

Ces données sont consignées dans les rapports annuels de l'Observatoire national de la délinquance et des réponses pénales (ONDPR). Il convient de porter à la connaissance du Conseil d'État les *« Éléments de connaissance sur la fraude aux documents et à l'identité »* communiqués dans chacun de ces rapports, qui sont disponibles pour les années 2013, 2014 et 2015 (pièces n° 12 à 14). Chacun de ces rapports comporte un tableau intitulé : « *Les différents types de documents français interceptés selon la nature de la fraude en France* ».

En premier lieu, on constatera que le nombre total de faux documents, tous types de fraudes et tous types de documents confondus, est particulièrement faible pour un pays de soixante-six millions d'habitants : 10 451 en 2013, 6 429 en 2014 et 6 199 en 2015.

En second lieu, on rappellera que le décret attaqué ne se propose pas de lutter contre tous les types de fraude — rien n'est prévu contre la contrefaçon, la falsification ou encore l'usage frauduleux — ni ne sera utile relativement à tous les types de documents — sont notamment exclus les titres de séjour et les visas.

Aussi, le dispositif prévu par le décret attaqué est déjà largement en vigueur s'agissant du passeport. À titre de comparaison, la mise en place du passeport biométrique n'a pas substantiellement affecté le nombre de fraudes à l'obtention de passeports, puisque le nombre de cas reste stable : 231 en 2013, 189 en 2014 et 208 en 2015. L'unique utilité prétendue du fichier TES sera donc de lutter contre la fraude relative aux cartes nationales d'identité, qui ne représente que 334 cas individuels pour 2013, 315 cas pour 2014 et 279 pour 2015.

Il n'est au demeurant pas démontré que le fichier TES sera efficace dans tous les cas d'obtention frauduleuse, puisqu'il convient de distinguer l'obtention initiale du document de son renouvellement. Ainsi, à l'égard de l'obtention initiale, le fichier TES ne sera d'aucune utilité dans la mesure où il ne contiendra aucune information de référence relative à la personne faisant une première demande. Autrement dit, le décret attaqué ne permettra en réalité de lutter que contre le cas très particulier de l'enregistrement sous une double identité : une même personne cherchant à obtenir deux titres d'identité sous deux noms différents.

Il faut donc considérer que ça n'est pas même contre trois cents cas frauduleux par an que le fichier TES permettra de lutter, mais contre quelques dizaines seulement.

Le mise en œuvre de ce fichier revient donc, si l'on développe les arguments déclarés par ses promoteurs eux-mêmes, à organiser le fichage biométrique d'une population de soixante-six millions de Français pour lutter — sans aucune garantie d'efficacité — contre une fraude de l'ordre de quelques dizaines de cas potentiellement litigieux par an.

Le décret attaqué viole donc de façon grave et indiscutable le principe de proportionnalité.

B. Sur le Règlement général sur la protection des données (RGPD)

Le Règlement général 2016/679 de l'Union européenne sur la protection des données personnelles (RGPD) entrera en vigueur le 25 mai 2018. Il s'appliquera indifféremment aux entités de droit public et privé, à l'intérieur et à l'extérieur de l'Union européenne, dès lors qu'elles traitent des données personnelles de résidents européens.

Le RGPD ayant été adopté par le Conseil et le Parlement européen le 27 avril 2016, soit six mois avant le décret attaqué, le rédacteur de ce dernier ne pouvait en ignorer l'existence. Pourtant, le décret porte au moins trois violations lourdes du RGPD : il organise la collecte et le traitement de données biométriques hors du cadre posé par le législateur européen (1) ; il ne répond pas à l'obligation de

sécurisation des données personnelles imposée par le RGPD (2) ; et enfin, il n'a été pas procédé à l'analyse d'impact requise (3).

1. **Sur le traitement non autorisé de données biométriques**

Le RGPD dispose, en son article 9, alinéa 1er :

> *Le traitement des données à caractère personnel qui révèle l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que* ***le traitement 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* ***sont interdits****.*

En dehors du cas où le *« consentement explicite »* de la personne a été recueilli, un certain nombre d'exceptions sont prévues, notamment en matière de droit du travail, de préservation des *« intérêts vitaux »* de la personne, dans le cadre d'associations ou de fondations, ou encore s'agissant de données déjà rendues publiques, en matière juridictionnelle, médicale, de santé publique, ou pour des besoins d'archivage.

En tout état de cause, la collecte de *« l'image numérisée du visage et celle des empreintes digitales »* de l'ensemble de la population française, prévue au paragraphe i) de l'article 2 du décret attaqué, ne correspond à aucune des exceptions listées ci-avant.

L'image numérisée du visage et celle des empreintes digitales correspondent pourtant à la définition des données biométriques au sens du RGPD :

> ***« données biométriques »****, les données à caractère personnel résultant d'un traitement technique spécifique, relatives aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique, qui permettent ou confirment son identification unique, telles que des* ***images faciales*** *ou des* ***données dactyloscopiques*** *;* (RGPD, article 4, paragraphe 14)

Nulle part le décret attaqué ne prévoit que soit recueilli le *« consentement explicite »* des Français avant la collecte de leurs données biométriques. Le paragraphe i) de l'article 2 du décret attaqué constituera donc, dès l'entrée en vigueur du RGPD, une violation grave et indiscutable de celui-ci.

2. **Sur la sécurité du traitement de données personnelles**

L'article 32 du RGPD dispose :

> 1. *Compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement* ***ainsi que des risques****, dont le degré de probabilité et de gravité varie,* ***pour les***

***droits et libertés des personnes physiques**, le responsable du traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées afin de **garantir un niveau de sécurité adapté au risque** (…)*

2. *Lors de l'évaluation du niveau de sécurité approprié, **il est tenu compte en particulier des risques que présente le traitement**, résultant notamment de la destruction, de la perte, de l'altération, de la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou de l'accès non autorisé à de telles données, de manière accidentelle ou illicite. (…)*

S'agissant des données collectées en application du décret attaqué, le risque est maximal : on n'ose imaginer les conséquences pour chacun d'entre nous en cas de piratage, de falsification ou simplement de compromission d'un fichier central contenant l'identité, les coordonnées, le visage et les empreintes digitales de pratiquement toute la population française !

Il découle de cette évidence qu'une application responsable de l'article 32 précité du RGPD aurait dû conduire le pouvoir réglementaire à adopter les mesures de sécurisation les plus élevées afin de protéger les données ultra-sensibles qui seront regroupées par l'administration dans le fichier TES.

Or il n'en n'est rien : à aucun moment, en aucun article le décret attaqué ne préconise la moindre mesure de sécurité concrète. Que ce soit au plan technique – les dispositifs informatiques à mettre en place – ou en matière organisationnelle – les procédures et les garde-fous permettant d'éviter le pire –, rien n'est prévu, rien n'est énoncé qui indique que les traitements issus du décret attaqué seront conformes à l'article 32 du RGPD. Par ce défaut de sécurisation, le décret attaqué fait courir à l'ensemble des Français un risque élevé de vol d'identité alors qu'il est justement censé, selon les dires de ses rédacteurs, lutter contre ce risque !

En outre, le décret attaqué prévoit la fourniture d'accès au fichier TES au bénéfice de nombreux services de l'État et organisations internationales sans jamais indiquer quels dispositifs de sécurisation de ces accès permettront de limiter les risques de compromission. Cette pratique, matérialisée notamment aux articles 4, 5, 6 et 7 du décret attaqué, constitue une violation manifeste de l'article 25 du RGPD, qui dispose que des mesures techniques et organisationnelles doivent être prises qui *« garantissent que, par défaut, les données à caractère personnel **ne sont pas rendues accessibles à un nombre indéterminé de personnes physiques sans l'intervention de la personne physique concernée** »*.

De même, les durées de conservation des données sont fixées par le décret attaqué sont supérieures à la durée de validité des titres émis, et ce sans explication ni justification en fait ou en droit de la part du pouvoir réglementaire. Le RGPD exige pourtant, dès le considérant 39 de son préambule, que *« la durée de conservation des données soit **limitée au strict minimum** »*.

Qu'il s'agisse de la sécurisation du fichier TES en lui-même, de celle de la transmission des données personnelles des Français entre services de l'État ou de la durée de conservation de ces données, chaque mesure prévue par le décret attaqué constitue une violation du RGPD.

3. Sur les analyses d'impact relatives à la protection de la vie privée

L'article 35 du RGPD prévoit qu'une analyse d'impact relative à la protection des données est requise *« **avant le traitement** »* (alinéa 1er), en cas de *« traitement **à grande échelle** de **catégories particulières de données** visées à l'article 9, paragraphe 1 »* (alinéa 3).

Comme vu *supra*, les données biométriques, au nombre desquelles la photographie du visage et des empreintes digitales, sont spécifiquement mentionnées par les *« catégories particulières »* de l'article 9, paragraphe 1 du RGPD.

En outre, l'article 36 du RGPD impose la consultation de l'autorité de contrôle, c'est-à-dire de la Commission nationale Informatique et libertés (CNIL), préalablement à tout traitement qui *« présenterait un **risque élevé** si le responsable du traitement ne prenait pas de mesures pour atténuer le risque »*.

Il est précisé au considérant n° 83 du préambule du RGPD que l'objectif d'une telle analyse d'impact est de *« **garantir la sécurité** et de **prévenir tout traitement effectué en violation** »* du RGPD. Le raisonnement du législateur européen est clair : dès qu'un traitement de données peut être considéré soit *« à grande échelle »*, soit *« à risque élevé »*, une analyse d'impact devrait être réalisée en amont. L'objectif est tout aussi limpide : *« adopter des règles internes et mettre en œuvre des mesures qui respectent, en particulier, les principes de **protection des données dès la conception** et de **protection des données par défaut** »*.

Dès lors, la création même du fichier TES constitué par le décret attaqué aurait dû être précédée, dans un souci de conformité, d'une analyse d'impact sur la protection des données personnelles des Français.

L'entrée en vigueur du décret attaqué, si elle précède celle du RGPD, est néanmoins postérieure à sa parution. Dans un souci de conformité au futur règlement européen, le pouvoir réglementaire aurait donc pu réaliser l'analyse d'impact prévue par le nouveau texte. Peut-être conscient de l'incompatibilité profonde entre le futur cadre européen en matière de données personnelles et la teneur du décret attaqué, il n'en n'a rien fait.

Pourtant, dès le 25 mai 2018 et sans qu'il soit besoin de procéder à une transposition en droit français, le RGPD s'imposera non seulement à toutes les organisations de droit privé ou public, mais également au législateur et au pouvoir réglementaire français.

Dès le 25 mai 2018, donc, et nonobstant tous les arguments relatifs à sa constitutionnalité ou à sa légalité interne ou externe, le décret attaqué portera une violation manifeste et indiscutable du droit de l'Union européenne.

La collecte de données biométriques aux simples fins d'établissement d'un titre d'identité, sans mesure de sécurisation ni de protection particulière et sans analyse d'impact préalable, sera interdite dans l'Union européenne. Le décret attaqué devra donc être retiré ou annulé.

∴

Il résulte de tout ce qui précède ainsi que des moyens, arguments et demandes formulés initialement que le 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 est contraire à la Constitution, à la Convention européenne des droits de l'homme, au Règlement général sur la protection des données et à la loi.

Le décret entrepris sera donc annulé dans l'ensemble de ses dispositions.

PAR CES MOTIFS

ET TOUS AUTRES À PRODUIRE, DÉDUIRE, OU SUPPLÉER AU BESOIN, MÊME D'OFFICE,

Il est demandé au Conseil d'État de :

- ANNULER le 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 ;

- CONDAMNER l'État à verser à Monsieur Gaspard KOENIG la somme de mille cinq cents euros, et à l'association GENERATIONLIBRE la somme de mille cinq cents euros, au titre de l'article L. 761-1 du Code de justice administrative.

BORDEREAU DES PIÈCES

- **Pièce n° 12 :** ONDPR, Éléments de connaissance sur la fraude aux documents et à l'identité, 2013 ;
- **Pièce n° 13 :** ONDPR, Éléments de connaissance sur la fraude aux documents et à l'identité, 2014 ;
- **Pièce n° 14 :** ONDPR, Éléments de connaissance sur la fraude aux documents et à l'identité, 2015.

PIÈCE N° 12

PIÈCE N° 13

PIÈCE N° 14