## Dépôt de plainte

En France, le décret en Conseil d'État n°2016-1460 du 28 octobre 2016 (Journal officiel de la République française n°0254 du 30 octobre 2016) a autorisé la création d'un traitement de données à caractère personnel relatif aux passeports et aux cartes nationales d'identité : le fichier dit Titres électroniques sécurisés (« TES »). Ce fichier commun pour les passeports et les cartes d'identité enregistre des données personnelles du demandeur ou du titulaire du titre dont notamment, selon l'article 2 dudit décret : le nom de famille, le ou les prénoms, la date et le lieu de naissance, le sexe, la couleur des yeux, la taille, les données relatives à sa filiation, l'image numérisée du visage, l'image numérisée des empreintes digitales et l'image numérisée de la signature du demandeur. Ainsi, la mise en œuvre de ce fichier centralise sur un même support des données personnelles de 60 millions de citoyens français, dont des données biométriques particulièrement sensibles. Il constitue une ingérence dans la vie privée des ressortissants français qui est disproportionnée et inadéquate par rapport au but poursuivi en violation du droit de l'Union Européenne. Par requête en date du 14 novembre 2016, Monsieur Gaspard KOENIG et l'association Génération Libre ont saisi le Conseil d'État français aux fins d'annuler pour excès de pouvoir ledit décret. Par un arrêt en date du 18 octobre 2018, le Conseil d'État a rejeté ces demandes. Le décret contesté, validé par la décision du Conseil d'État querellée méconnait les engagements européens précités en ce qu'il viole la protection des données personnelles et le droit au respect de la vie privée des ressortissants français. De surcroît, l'accès aux données collectées est prévu à d'autres fins de police administrative ou judiciaire, dans les cas de prévention ou de répression des atteintes aux intérêts fondamentaux de la Nation et du terrorisme. En second lieu, il n'est pas avéré que la constitution de ce fichier soit le seul moyen pour parvenir à cette fin. La CNIL propose d'autres moyens moins coercitifs et intrusifs. En effet, les finalités de sécurisation de la délivrance de titres, de simplification de la procédure et de lutte contre la fraude peuvent être réalisées par d'autres mesures moins contraignantes comme cela ressort de l'avis de la CNIL qui préconise la conservation des données biométriques brutes sur un support individuel exclusivement détenu par la personne. Il en va de même de la conservation des données biométriques brutes qui pour des raisons de sécurité pourrait être utilement remplacée par des gabarits de celles-ci. De plus,le Contrôleur européen de la protection des données (CEPD), dans son avis n°7/2018 du 10 aout 2018 sur la proposition de règlement relatif au renforcement de la sécurité des cartes d'identité des citoyens de l'Union et d'autres documents, considère que le traitement de deux types de données biométriques, image faciale et deux empreintes digitales pour les cartes d'identité n'est pas justifié.
En effet, le CEPD soutient que l'objectif de la Commission européenne de renforcer les normes de sécurité applicables aux cartes d'identité et aux titres de séjour pourrait être atteint par une approche moins intrusive.

Le CEPD rappelle que la nécessité constitue un principe essentiel dans l'évaluation de la limitation des droits fondamentaux et l'évaluation de la proportionnalité de cette limitation.
Or, le CEPD considère que la nécessité de traiter trois données biométriques, image faciale et deux empreintes digitales, dans la carte d'identité n'est pas justifiée.
En effet, le CEPD énonce la diminution constante des cartes d'identité frauduleuses depuis plusieurs années selon les statistiques d'analyses de risque de fraude établies par l'Agence européenne de garde-frontières et de garde-côtes (Frontex). A ce jour, le nombre de carte d'identité frauduleuse est même faible.
Contrairement à l'article 32 du RGPD, 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. 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. 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 ». L'autorité de contrôle et de régulation des données personnelles en France, la Commission nationale de l'informatique et des libertés (CNIL), dans ses deux avis relatifs à ce fichier publiés, les délibérations n°2016-292 du 29 septembre 2016 et n°2017-058 du 16 mars 2017, a émis de nombreuses réserves quant à la création de ce fichier TES.LA CNIL considère en effet que « la mesure envisagée entrainerait des conséquences contraires à l'objectif de simplification administrative sans pouvoir être justifiée par l'amélioration de la lutte contre la fraude documentaire ». Selon la CNIL, les risques encourus par la création d'un tel fichier TES sont donc totalement contraires à ceux visés par ses finalités initiales. Dans le même sens, le rapport d'audit de sécurité du système TES élaboré conjointement par l'Agence nationale de la sécurité des systèmes d'information (ANSSI) et la Direction interministérielle du numérique et du système d'information et de communication de l'État (DINSIC) met en évidence les vulnérabilités quant à la sécurité de ce fichier TES. Des garanties sont nécessaires afin de s'assurer que les données ne soient pas utilisées à d'autres fins que leurs finalités initiales. Des analyses d'impact devraient être réalisées et suivies conformément à l'article 35 du RGPD. Il y a un niveau d'insécurité au niveau de l'accessibilité et de la traçabilité des données contrairement aux articles 44 et suivants du RGPD. De nombreux agents peuvent accéder aux données personnelles enregistrées. Il est fait appel à de nombreux sous-traitants, une insécurité des transferts des données hors l'Union européenne. Des données biométriques traitées sans consentement contrairement à article 9 du RGPD.

Ainsi, en France, la protection des personnes physiques à l'égard du traitement de leurs données à caractère personnel n'est pas respecté par la validation du décret n°2016-1460 du 28 octobre 2016 par le Conseil d'Etat par sa décision du 18 octobre 2018. Ce droit fondamental est énoncé dans :

- le Traité sur le fonctionnement de l'Union européenne, notamment son article 16 ;
- la Charte des droits fondamentaux de l'Union européenne, notamment ses articles 7, 8 et 52 ;
- le 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 (RGPD), abrogeant la directive 95/46/CE