

ASSEMBLEE DE CORSE

1 ERE SESSION EXTRAORDINAIRE DE 2021

REUNION DES 28 ET 29 JANVIER 2021

RAPPORT DE MONSIEUR
LE PRESIDENT DU CONSEIL EXECUTIF DE CORSE

**DUMANDA D'ABRUGAZIONI DI I TRE DICRETI
NU 2020-1510, NU 2020-1511 E NU 2020-1512 DI U 2 DI
DICEMBRE DI U 2020 RILATIVI A I TRATTAMENTI DI I
DATI PARSUNALI IN U QUATRU DI I CARTILLAGHJI
DETTI DI SICUREZZA PUBBLICA EASP, PASP E GIPASP
DEMANDE D'ABROGATION DES TROIS DÉCRETS
N° 2020-1510, N° 2020-1511 ET N° 2020-1512
DU 2 DÉCEMBRE 2020 RELATIFS AUX TRAITEMENTS DES
DONNÉES PERSONNELLES AU SEIN DES TROIS FICHIERS
DITS "DE SECURITE PUBLIQUE" EASP, PASP ET GIPASP**

RAPPORT DU PRESIDENT DU CONSEIL EXECUTIF DE CORSE

Le présent rapport a pour objet de mettre en évidence l'impact sur les libertés publiques des trois décrets n° 2020-1510, n° 2020-1511 et n° 2020-1512 du 2 décembre 2020 (**Annexe I, II et III, ci-après « les Décrets »**) étendant les possibilités de traitement de données personnelles au sein de trois fichiers dits de « sécurité publique » : le fichier des enquêtes administratives ([EASP](#)) et le fichier de prévention des atteintes à la sécurité publique (le [PASP](#)), tous deux gérés par la police et créés en 2009, et le fichier de Gestion de l'information et prévention des atteintes à la sécurité publique (« [GIPASP](#) »), l'équivalent du PASP pour la gendarmerie, créé en 2011.

Ces trois fichiers sont particulièrement sensibles ; en ce qu'ils autorisent policiers et gendarmes à faire mentionner les opinions politiques, appartenances syndicales, des convictions philosophiques ou religieuses, ou encore des données de santé au nom de la sûreté de l'Etat, dans des fichiers où sont mentionnées des atteintes à la sécurité publique. Les identifiants, photos et commentaires postés sur les réseaux sociaux peuvent également y être indexés, tout comme les troubles psychologiques « *révélant une dangerosité particulière* ».

Les Décrets avaient fait l'objet de quatre recours demandant la suspension de l'exécution de ces textes, devant le Conseil d'Etat statuant en référé, sur le fondement de l'article L. 521-2 du Code de justice administrative (référé-liberté), par plusieurs confédérations syndicales et organisations professionnelles (Confédération Générale du Travail, Force ouvrière, la Fédération syndicale unitaire, l'Union syndicale Solidaires, le Syndicat de la magistrature, le Syndicat des avocats de France, le Groupe d'information et de soutien des immigrés et l'Union nationale des étudiants de France). D'autres associations (la Ligue des Droits de l'Homme, la Quadrature du Net) s'étaient joints aux recours ou avaient introduits d'autres recours similaires (Association VIA la voie du Peuple, Association Fondation Service politique).

Les recours soutenaient que les dispositions des Décrets contrevenaient notamment à la loi n° 78-17 du 6 janvier 1978 dite « loi informatique et liberté », notamment son article 6¹, à la Convention de sauvegarde des droits de l'homme et des libertés fondamentales (« CESDH ») et à la Constitution, en ce que les Décrets portaient une atteinte manifestement illégale à plusieurs libertés fondamentales : la liberté d'opinion, de conscience et de religion, la liberté syndicale, le droit à la vie privée et familiale...

¹ Article 6 : I. Il est interdit de traiter des 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.

II. Les exceptions à l'interdiction mentionnée au I sont fixées dans les conditions prévues par le 2 de l'article 9 du règlement (UE) 2016/679 du 27 avril 2016 et par la présente loi.

III. De même, ne sont pas soumis à l'interdiction prévue au I les traitements, automatisés ou non, justifiés par l'intérêt public et autorisés suivant les modalités prévues au II de l'article 31 et à l'article 32 ».

Aux termes de l'article 31 de la loi du 6 janvier 1978 : « (...) II. Ceux de ces traitements qui portent sur des données mentionnées au I de l'article 6 sont autorisés par décret en Conseil d'Etat pris après avis motivé et publié de la commission. Cet avis est publié avec le décret autorisant le traitement (...) ». Aux termes de l'article 90 de la même loi, applicable aux traitements de données à caractère personnel relevant de la directive 2016/680 du 27 avril 2016 : « 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 6, le responsable de traitement effectue une analyse d'impact relative à la protection des données à caractère personnel. / Si le traitement est mis en œuvre pour le compte de l'Etat, 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 33 ».

Par quatre ordonnances en date du 4 janvier 2021, le Conseil d'Etat a rejeté ces recours en considérant : « que le moyen tiré de ce que le décret attaqué porterait une atteinte disproportionnée au droit au respect de la vie privée au regard de l'absence de finalité claire et légitime, du caractère inadéquat et non pertinent des données collectées, du périmètre excessivement étendu de l'accès aux données et du caractère excessif de la durée de conservation des données n'est pas de nature, en l'état de l'instruction, à faire naître un doute sérieux sur la légalité du décret attaqué ».

Et : « Aucun des moyens n'apparaît donc de nature, en l'état de l'instruction, à faire naître un doute sérieux sur la légalité du décret attaqué. Les conclusions aux fins de suspension de son exécution doivent, par suite, être rejetées. » ²

Ainsi, le Conseil d'Etat a estimé que l'élargissement des fichiers de police ne portait pas une atteinte disproportionnée à la liberté d'opinion, de conscience et de religion ou à la liberté syndicale (**Cf. Annexe V**).

En conséquence, et même si un recours au fond a été engagé devant le Conseil d'Etat, les dispositions des Décrets sont applicables depuis le 5 décembre 2020.

Dans un premier temps, on s'attachera à en mettre en évidence les grandes lignes (I) avant de nous interroger sur les risques d'atteinte à l'exercice des libertés publiques (II), puis de conclure (III).

I. Analyse des principaux changements introduits par les décrets :

Historique

En 2008, la Direction de la Sécurité du Territoire et les Renseignements Généraux ont été supprimés et leurs missions ont été partagées entre la DCRI (maintenant DGSI, la direction générale de la sécurité intérieure) et la DGPN (direction générale de la police nationale). Les fichiers des anciens services ont été partagés entre la DCRI (qui les a récupérés dans le fichier CRISTINA) et la DGPN (dans un fichier alors nommé EDVIGE).

Une mobilisation historique sur l'étendue trop importante des informations contenues dans EDVIGE avait forcé le gouvernement à retirer le décret qui l'autorisait. Le gouvernement avait reculé et permis de fichier uniquement les « activités » des

personnes et non leurs opinions.

Douze ans après, cette barrière saute : PASP, GIPASP et EASP contiendront des éléments sur les « *opinions politiques* » et les « *convictions philosophiques et religieuses* », et plus seulement sur les activités politiques, religieuses et syndicales.

Les Décrets permettront aussi d'aller au-delà de la notion de « *menace à l'ordre public* » qui a fondé le PASP et le GIPASP. Pourront être fichées les personnes pouvant porter atteinte à la sûreté de l'État, du territoire ou des institutions de la République. Des notions plus vagues permettant un fichage plus aisé.

Les Décrets visent aussi à mieux surveiller l'activité des personnes morales et des groupements de fait, qui pourront être fichés comme le sont les personnes physiques.

² Ordonnances du Conseil d'Etat n° 447970, 447971 et 44972 en date du 4 janvier 2021, points 17 et 22.

Une disposition directement liée à la volonté du gouvernement de mieux surveiller les activités associatives.

Le fichage en fonction des opinions et des convictions religieuses

Les trois décrets portent sur les fichiers frères du renseignement territorial de la police (PASP) et la gendarmerie (GIPASP) et celui qui permet les enquêtes administratives (EASP) nécessaires pour la profession de magistrat, policier, surveillant pénitentiaire, policier municipal, agent de sécurité privé ou de la Hadopi.

Rappelons que le PASP et GIPASP ont un champ plus large que le Fichier des signalements pour la prévention de la radicalisation à caractère terroriste (FSPRT) qui vise les personnes radicalisées. En 2017, 43 500 personnes étaient fichées au PASP et 40 500 au GIPASP.

Des fichiers larges qui permettent aux forces de l'ordre de surveiller toute personne présentant une menace à l'ordre public (manifestants violents, hooligans...). Peuvent accéder au PASP et au GIPASP, les agents des services, mais également tous les policiers et gendarmes, ainsi que les procureurs (une nouveauté des décrets).

PASP et GIPASP sont les enfants du fichier Edvige. Un fichier qui, il y a une douzaine d'années, avait fait beaucoup de bruit, au point d'être retiré. À l'époque, les pétitionnaires reprochaient à ce fichier aux mains du renseignement territorial de permettre le recueil d'informations sur l'opinion des personnes fichées...

Le gouvernement avait reculé et permis de fichier uniquement les « *activités* » des personnes. Douze ans après, cette barrière saute : PASP, GIPASP et EASP contiendront des éléments sur les « *opinions politiques* » et les « *convictions philosophiques et religieuses* », et plus seulement sur les activités politiques, religieuses et syndicales¹.

¹ Modification de l'article R. 236-13 du Code de la sécurité intérieure

Article 3 du décret n° 2020-1510 du 2 décembre 2020 modifiant les dispositions du code de la sécurité intérieure relatives au traitement de données à caractère personnel dénommé « Enquêtes administratives liées à la sécurité publique » :
« Art. 3. - L'article R. 236-13 du même code est ainsi modifié : 1° Au premier alinéa, la référence : « 8 » est remplacée par la référence : « 6 » ; 2° Le 2° est remplacé par les dispositions suivantes : « **A des opinions politiques, des convictions philosophiques, religieuses ou une appartenance syndicale** » ; 3° Après le 2°, il est inséré un 3° ainsi rédigé : « **3° A des**

Les nouveaux décrets permettront aussi d'aller au-delà de la notion de « *menace à l'ordre public* » qui a fondé le PASP et le GIPASP. Pourront être fichées les personnes pouvant porter atteinte à la sûreté de l'État, du territoire ou des institutions de la République. Des notions plus vagues et qui permettent d'étendre le champ d'application des fichiers.

Les personnes morales et les groupements de fait pourront désormais être fichés comme le sont les personnes physiques. Nous verrons plus bas qu'une telle disposition est susceptible d'engendrer de nombreuses dérives.

Cette disposition est directement liée à une volonté générale du gouvernement de mieux surveiller les activités associatives. Ainsi, ce thème se retrouve dans le projet de loi contre le « séparatisme » (devenu projet « confortant les principes républicains »), qui sera examiné par le du Parlement cet hiver, et vise à renforcer les possibilités de contrôle et de dissolution des associations, qu'elles soient constituées sur le fondement de la loi de 1901 ou de loi de 1905 (association culturelles).

L'élargissement considérable des données susceptibles d'être recueillies et la surveillance des réseaux sociaux

Dans son avis² sur les fichiers, la CNIL note aussi que le décret va « étendre de manière très significative la liste des catégories de données susceptibles d'être collectées ».

Si l'on compare les deux versions de l'article, l'ampleur de l'élargissement des données susceptibles d'être recueillies dans les fichiers est impressionnante.

Ancien article R. 236-12 de Code de la sécurité intérieure :

« Peuvent être enregistrées dans le traitement mentionné à l'article R. 236-11, dans le respect des dispositions de l'article 6 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et dans la stricte mesure où elles sont nécessaires à la poursuite de la finalité mentionnée au second alinéa de l'article R. 236-11, les catégories de données à caractère personnel suivantes :

- 1° Motif de l'enregistrement ;*
- 2° Informations ayant trait à l'état civil, à la nationalité et à la profession, adresses physiques, numéros de téléphone et adresses électroniques, origine géographique (c'est-à-dire : lieu de naissance, lieux de résidence et zones d'activité) ;*
- 3° Signes physiques particuliers et objectifs, photographies ;*
- 4° Titres d'identité ;*
- 5° Immatriculation des véhicules ;*
- 6° Informations patrimoniales ;*
- 7° Activités publiques, comportement et déplacements ;*
- 8° Agissements susceptibles de recevoir une qualification pénale ;*
- 9° Personnes entretenant ou ayant entretenu des relations directes et non fortuites avec l'intéressé.*

Le traitement ne comporte pas de dispositif de reconnaissance faciale à partir de la photographie. »

Nouvelle rédaction de l'article R. 236-12 :

« Peuvent être enregistrées dans le traitement mentionné à l'article R. 236-11, dans le respect des dispositions de l'article 4 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et dans la stricte mesure où elles sont nécessaires à la poursuite des finalités mentionnées à l'article R. 236-11, les catégories de données à caractère personnel suivantes :

I.- Données concernant la personne physique pouvant porter atteinte à la sécurité publique ou à la sûreté de l'Etat :

- 1° Eléments d'identification :*
 - a) Nom ;*
 - b) Prénoms ;*
 - c) Alias ;*
 - d) Date et lieu de naissance ;*

2 Délibération CNIL n° 2020-064 du 25 juin 2020 portant avis sur un projet de décret 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 » (demande d'avis n° 19013316)

- e) *Nationalité ;*
- f) *Signes physiques particuliers et objectifs ;*
- g) *Photographies ;*
- h) *Documents d'identité (type, numéro, validité, autorité et lieu de délivrance) ;*
- i) *Origine géographique (lieux de résidence et zones d'activité) ;*
- 2° *Coordonnées :*
 - a) *Numéros de téléphone ;*
 - b) *Adresses postales et électroniques ;*
 - c) *Identifiants utilisés (pseudonymes, sites ou réseaux concernés, autres identifiants techniques), à l'exclusion des mots de passe ;*
 - d) *Adresses et lieux fréquentés ;*
- 3° *Situation :*
 - a) *Situation familiale ;*
 - b) *Formation et compétences ;*
 - c) *Profession et emplois occupés ;*
 - d) *Moyens de déplacement (moyens utilisés, immatriculation des véhicules, permis de conduire) ;*
 - e) *Situation au regard de la réglementation de l'entrée et du séjour en France ;*
 - f) *Éléments patrimoniaux ;*
- 4° *Motifs de l'enregistrement ;*
- 5° *Activités susceptibles de porter atteinte à la sécurité publique ou à la sûreté de l'Etat :*
 - a) *Activités publiques ou au sein de groupements ou de personnes morales ;*
 - b) *Comportement et habitudes de vie ;*
 - c) *Déplacements ;*
 - d) *Activités sur les réseaux sociaux ;*
 - e) *Pratiques sportives ;*
 - f) *Pratique et comportement religieux ;*
- 6° *Facteurs de dangerosité :*
 - a) *Lien avec des groupes extrémistes ;*
 - b) *Éléments ou signes de radicalisation, suivi pour radicalisation ;*
 - c) *Données relatives aux troubles psychologiques ou psychiatriques obtenues conformément aux dispositions législatives et réglementaires en vigueur ;*
 - d) *Armes et titres afférents ;*
 - e) *Détention d'animaux dangereux ;*
 - f) *Agissements susceptibles de recevoir une qualification pénale ;*
 - g) *Antécédents judiciaires (nature des faits et date) ;*
 - h) *Fiches de recherche ;*
 - i) *Suites judiciaires ;*
 - j) *Mesures d'incarcération (lieu, durée et modalités) ;*
 - k) *Accès à des zones ou des informations sensibles ;*
- 7° *Facteurs de fragilité :*
 - a) *Facteurs familiaux, sociaux et économiques ;*
 - b) *Régime de protection ;*
 - c) *Faits dont la personne a été victime ;*
 - d) *Comportement auto-agressif ;*
 - e) *Addictions ;*
 - f) *Mesures administratives ou judiciaires restrictives de droits, décidées ou proposées ;*
- 8° *Indication de l'enregistrement ou non de la personne dans les traitements de données à caractère personnel suivants :*
 - a) *Le traitement d'antécédents judiciaires mentionné aux articles R. 40-23 et suivants du Code de procédure pénale ;*

- b) *Le système informatique national N-SIS II mentionné aux articles R. 231-5 et suivants du présent code ;*
- c) *Le traitement automatisé de données à caractère personnel dénommé Gestion de l'information et prévention des atteintes à la sécurité publique mentionné aux articles R. 236-21 et suivants du présent code ;*
- d) *Le fichier des personnes recherchées prévu par le décret n° 2010-569 du 28 mai 2010 portant création du fichier des personnes recherchées ;*
- e) *Le traitement automatisé de données à caractère personnel dénommé FSPRT mentionné au 12 de l'article 1^{er} du décret n° 2007-914 du 15 mai 2007 modifié pris pour l'application du I de l'article 30 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ;*
- f) *Le traitement automatisé des données relatives aux objets et véhicules volés ou signalés.*

II. Données concernant les personnes physiques 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, notamment ses parents et ses enfants, dans la stricte mesure où ces données sont nécessaires pour le suivi de la personne concernée et dans la limite des catégories mentionnées aux 1°, 2°, 3° et 5° à l'exception du c du I.

III. Données concernant les victimes des agissements de la personne physique pouvant porter atteinte à la sécurité publique ou la sûreté de l'Etat, dans la stricte mesure où ces données sont nécessaires à la protection des intérêts de la victime et à la prévention de la réitération de faits par la personne concernée et dans la limite des catégories mentionnées aux 1°, 2°, 3°, 5° à l'exception du c du I et au c du 7° du I.

IV. - Données concernant les personnes physiques entretenant ou ayant entretenu des relations directes et non fortuites avec la personne morale ou le groupement pouvant porter atteinte à la sécurité publique ou à la sûreté de l'Etat, ou victimes des agissements de ces personnes morales et groupements, dans la stricte mesure où ces données sont nécessaires à leur suivi et dans la limite des catégories mentionnées aux 1°, 2°, 3°, 5° à l'exception du c du I, et, concernant les victimes, au c du 7° du I. »

La variété et l'étendue du type de données recueillies et le croisement avec d'autres fichiers (TAJ, FPR, FSPRT, API-PNR, système des permis de conduire...) - n'en déplaise au Conseil d'Etat qui a rejeté l'interconnectivité des fichiers comme moyen efficace dans les recours précités - est alarmant.

Parmi les éléments saillants notons également que les services de police et de gendarmerie pourront fichier des éléments sur les « *données de santé révélant une dangerosité particulière* » des personnes et les « *données relatives aux troubles psychologiques ou psychiatriques obtenues conformément aux dispositions législatives et réglementaires en vigueur* ». Les données de santé avaient été exclues dans le PASP et le GIPASP après le tollé sur le fichier EDVIGE.

La commission souhaitait que le gouvernement précise les catégories « *comportement et habitudes de vie* », « *déplacements* » ou encore « *pratiques sportives* », mais il n'a pas pris en compte son avis.

Le nouveau décret accroît les connexions avec d'autres fichiers de police (TAJ, FPR, FSPRT, API-PNR, système des permis de conduire...). Le décret prévoit aussi le fichage de la « *pratique et des comportements religieux* » ainsi que les « *activités sur*

les réseaux sociaux ».

Les fonctionnaires pourront aussi recueillir les identifiants et pseudonymes sur les réseaux sociaux (mais pas les mots de passe). Dans le cadre du fichier EASP sur les enquêtes administratives, toute personne souhaitant avoir une habilitation devra d'ailleurs fournir ses pseudos, y compris Twitter.

Selon la CNIL « *seules les informations mises volontairement en ligne par leurs propriétaires en source ouverte, sans qu'elles soient conditionnées à un accès particulier, pourront être consultées et collectées* ». Pour les données non publiques, il faudra passer par les services de renseignement.

La reconnaissance faciale

Le ministère a précisé à la CNIL « *que les informations collectées porteront principalement sur les commentaires postés sur les réseaux sociaux et les photos ou illustrations mises en ligne* ».

La CNIL tient à souligner que le résultat devra être recoupé et qu'il « *ne suffira en aucune manière à lui seul à fonder une décision à l'égard de la personne, et aucune conséquence directe n'affectera la personne concernée* ». Une reconnaissance qui n'est pas encore développée dans l'application.

Il faut noter que l'ancienne rédaction de l'article R. 236-12 de Code de la sécurité intérieure excluait explicitement en son dernier alinéa le recours à la reconnaissance faciale « *Le traitement ne comporte pas de dispositif de reconnaissance faciale à partir de la photographie* », et que ces dispositions ont été supprimées.

La CNIL précise enfin que pour le PASP et le GIPASP, le nouveau décret « *vise à permettre de tenir compte de l'évolution de certaines pratiques dans l'utilisation de ce traitement et, ce faisant, de les régulariser.* » Il n'est pas forcément très rassurant de voir qu'un décret court derrière une pratique policière en cours.

II. Risques pour les libertés publiques :

Un rapport³ de 2018 permet de bien saisir le fonctionnement de ces fichiers de renseignement : en 2017, le PASP comportait 43 446 notes sur des individus, répartis autour d'une demi-douzaine de thèmes qu'on pourrait résumer ainsi :

- manifestations illégales ;
- violences et dégradations liées à des contestations idéologiques ;
- violence et vandalisme lors de manifestations sportives ;
- violences liées aux économies souterraines ;
- discours prônant la haine, agressions, stigmatisations envers certaines communautés ;
- radicalisation, prosélytisme virulent, velléités de départ à l'étranger en zone de combat ;
- pressions sectaires.

Ces notes pouvaient contenir des informations particulièrement détaillées :

³ <https://www.interieur.gouv.fr/Publications/Securite-interieure/Prevention-des-atteintes-a-la-securite-publique-traitement-des-donneespersonnelles-des-mineurs>

Ce rapport annuel n'a d'ailleurs été réalisé pour les fichiers PASP et GIPASP qu'en 2017 par le référent national et non chaque année, en contradiction avec l'article R. 236-15 alinéa 5 du Code de la sécurité publique.

profession, adresses physiques, email, photographies, activités publiques, comportement, déplacements...

Fichage généralisé des manifestants

Jusqu'à présent, les fichiers de renseignement de la police (PASP) et de la gendarmerie (GIPASP) ne concernaient que des **personnes physiques** considérées comme dangereuses par les autorités. Nouveauté importante introduite par les Décrets, les fichiers pourront aussi concerner des personnes morales ou des « *groupements* ». On imagine qu'il s'agira d'associations, des groupes Facebook, de squats, de ZAD ou même de manifestations.

Si une fiche est ouverte pour une manifestation, le PASP et le GIPASP permettent aussi de lister les personnes « *entretenant ou ayant entretenu des relations directes et non fortuites* » avec ce « *groupement* ». Jusqu'à présent, les fiches du PASP et du GIPASP ne pouvaient lister l'entourage des « *personnes dangereuses* » que de façon succincte, sur la fiche principale de la personne dangereuse. Désormais, si la police le juge nécessaire, **chaque membre de l'entourage pourra avoir une fiche presque aussi complète** que celle des personnes dangereuses (activités en ligne, lieux fréquentés, mode de vie, photo...).

Ces deux évolutions semblent officialiser une pratique (jusqu'alors illégale) qui commençait à apparaître dans le rapport de 2018 précité : « *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 interpellées alors qu'il n'est fait état dans la note d'aucun fait personnel qui leur est reproché* ». C'est ainsi l'ensemble des participants (« *ayant entretenu une relation directe et non fortuite* ») à une manifestation (« *groupement* » considéré comme dangereux) qui pourraient se voir attribuer une fiche particulièrement détaillée sur la base d'informations obtenues par la police sur le terrain (vidéos captées par drones et caméra mobile, par exemple) ou sur les réseaux sociaux.

Fichage automatisé

Les trois décrets augmentent considérablement la variété et l'ampleur des informations pouvant être enregistrées. Sont visées les « *habitudes de vie* » et les « *activités en ligne* ».

Dans son avis préalable⁴, la CNIL souligne que « *l'ensemble des réseaux sociaux est concerné* », « *les données sont à ce titre collectées sur des pages ou des comptes ouverts* » et « *porteront principalement sur les commentaires postés sur les réseaux sociaux et les photos ou illustrations mises en ligne* ».

Ceci constitue une forme de surveillance devenue monnaie courante à défaut d'être encadrée dans la loi, et d'autant plus dangereuse qu'elle peut facilement être automatisée.

⁴ Délibération CNIL n° 2020-064 du 25 juin 2020 portant avis sur un projet de décret 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 » (demande d'avis n° 19013316)

Inquiète, la CNIL demandait à « *exclure explicitement la possibilité d'une collecte automatisée de ces données* ». Le gouvernement a refusé d'ajouter une telle réserve, souhaitant manifestement se permettre de telles techniques, qu'il s'est déjà autorisé en d'autres matières (notamment en matière de surveillance fiscale)⁵.

Opinions politiques et données de santé

Comme il a été évoqué ci-dessus, les notes individuelles peuvent désormais contenir des informations qui relèvent « *des **opinions politiques, des convictions philosophiques, religieuses ou une appartenance syndicale*** » là où, avant, seules pouvaient être enregistrées des informations se rattachant à « *des **activités politiques, philosophiques, religieuses ou syndicales*** ».

Une digue très importante vient de tomber : on peut désormais être dans un fichier de police à raison de ses seules opinions, sans qu'aucun acte positif ne soit requis.

On passe d'une logique de fichage d'activités à celle d'un recensement d'opinion. S'agissant des personnes considérées comme dangereuses, le fichier pourra désormais recueillir des **données de santé** supposées « *révéler une dangerosité particulière* » : « *addictions* », « *troubles psychologiques ou psychiatriques* », « *comportement auto-agressif* ». La CNIL souligne qu'il ne s'agira pas d'une information « *fournie par un professionnel de santé [mais] par les proches, la famille ou l'intéressé lui-même* ».

Difficile de comprendre en quoi la police aurait besoin d'une telle variété de données aussi sensibles, si ce n'est pour faire pression et abuser de la faiblesse de certaines personnes.

Fichage des victimes et des enfants

Le PASP et le GIPASP peuvent désormais contenir des fiches détaillées sur les « *victimes* » des personnes considérées comme dangereuses (sans que cette notion de « *victime* » ne renvoie à une notion pénale, étant interprétée librement par les agents).

Plus inquiétant encore : alors que, depuis leur origine, le PASP et le GIPASP interdisaient de ficher des enfants de moins de 13 ans, les nouveaux décrets semblent désormais indiquer que seuls les mineurs considérés comme dangereux bénéficieront de cette protection d'âge. Ainsi, en théorie, plus rien n'empêche la police de consigner dans le fichier des informations relatives à *un* enfant de 5 ans ou de 10 ans se trouvant dans l'entourage d'une personne considérée comme dangereuse ou parce qu'il se trouvait dans une manifestation qui a dégénéré.

Recoupement de fichiers

Le rapport de 2018 précité explique que « *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 [et 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,*

⁵ Loi de finances 2019 article 153.

membres du groupe, antagonistes...) ».

Cette constitution de graphes sociaux fait directement écho à l'entourage des « *groupements* » décrit plus haut. Mais ce commentaire renvoie aussi à une autre réalité, décrite par la CNIL dans son avis préalable : de nombreuses catégories d'informations comprises dans les trois fichiers « *seront alimentées manuellement par d'autres traitements* » - les agents nourriront les fichiers PASP, GIPASP et EASP en allant manuellement chercher des informations dans d'autres fichiers. Pour leur faciliter le travail, les nouveaux décrets prévoient que les notes individuelles mentionneront si la personne concernée est aussi fichée dans l'un des 5 autres grands fichiers de police (TAJ, N-SIS II, fichier des personnes recherchées, FSPRT, fichiers des objets et véhicules volés ou signalés).

Reconnaissance faciale

Autre nouveauté facilitant considérablement le recoupement des fichiers : les décrets prévoient que le PASP, le GIPASP et l'EASP participent non seulement à la sécurité publique, mais désormais aussi à la « *sûreté de l'État* », qui est définie comme recouvrant les « *intérêts fondamentaux de la Nation* ». Il s'agit d'une notion très large, que la loi renseignement de 2015 a défini comme couvrant des choses aussi variées que « *les intérêts économiques et industriels majeurs de la France* », le respect des engagements internationaux pris par la France ou la lutte contre les manifestations non-déclarées et les attroupements. Un des intérêts de cette notion juridique est de donner accès aux photographies contenues dans le fichier TES, destiné à centraliser les photos de tout détenteur de passeport et de carte d'identité.

Une fois obtenues, les photographies pourront être ajoutées au PASP ou au GIPASP et, pourquoi pas, aussi au TAJ, où elles pourront être analysées par reconnaissance faciale.

D'ailleurs, les Décrets ont pris le soin de supprimer la mention qui, depuis leur origine, précisait que le PASP comme le GIPASP « *ne comporte pas de dispositif de reconnaissance faciale* ».

En lisant l'avis de la CNIL, on comprend que le projet initial prévoyait carrément d'ajouter un nouveau dispositif de reconnaissance faciale dans le PASP et le GIPASP, afin d'identifier automatiquement les fiches correspondant à la photographie d'une personne : « *l'interrogation par la photographie doit constituer une nouvelle possibilité d'interrogation du traitement (à l'instar du nom) [...] aux fins de déterminer si la personne dont la photographie est soumise figure déjà dans le traitement* ». Ce nouveau système n'apparaît plus dans les décrets publiés, le gouvernement ayant sans doute préféré créer des ponts entre les différents dispositifs existants.

III. Conclusion

Alors que la proposition de loi n° 3452 relative à la sécurité globale, adoptée en première lecture à l'Assemblée Nationale le 24 novembre 2020, dite « *loi sécurité globale* », autorise des techniques de captation d'informations en masse (drones et caméras piétons), ces trois nouveaux décrets viennent en quelque sorte la compléter et concernent la façon dont ces informations pourront être exploitées et conservées, pendant dix ans.

Si, via la loi sécurité globale, tous les manifestants pourront être filmés en manifestation et que, via le fichier TAJ, une grande partie d'entre eux pourra être identifiée par reconnaissance faciale, le PASP et le GIPASP leur a déjà préparé une fiche complète où centraliser toutes les informations les concernant, sans que cette surveillance ne soit autorisée ni même contrôlée par un juge.

L'ensemble de ce système, aussi complexe qu'autoritaire, poursuit l'objectif décrit dans le récent livre blanc de la sécurité intérieure⁶: faire passer la surveillance policière à une nouvelle ère technologique avant les JO de 2024.

Il n'est pas besoin d'insister sur les risques que fera peser sur la société corse, qui plus est dans le contexte de crise sanitaire et économique actuelle, l'application mécanique de ces décrets, avec l'aggravation de tensions sociales à la clef. Des comportements policiers trop « zélés » pourraient engendrer des conséquences incontrôlables.

Des voix s'élèvent - assez timidement - au sein de la classe politique française contre cette tentation du « *tout sécuritaire numérique* » du gouvernement : on peut noter les questions écrites de Mme Esther Benbassa au sujet des Décrets, ou encore de Delphine Bathot.

Deux députés de la Corse ont manifesté leur vive opposition à ces textes :

- Jean-Félix Acquaviva, lors de la séance publique de l'Assemblée nationale du 9 décembre 2020, consacrée à l'examen du projet de loi relatif au parquet européen et à la justice pénale spécialisée, a ainsi mis en relief, à propos de ces décrets, que : « outre les personnes susceptibles de prendre part à des activités terroristes, pourraient être collectées des informations concernant les personnes susceptibles de porter atteinte à l'intégrité du territoire et aux institutions de la République, critères larges (...) dans lesquels viendra certainement se nicher de l'arbitraire » ;
- Paul-André Colombani, dans un courrier adressé au Ministre de l'Intérieur, le 6 janvier 2021, a de son côté fustigé « le spectre des dérives sécuritaires et de l'utilisation abusive du fichage policier conduisant à une nouvelle vague de répression injuste, abusive et généralisée de militants nationalistes (...) ; sur la forme il est insupportable de voir le Gouvernement prendre des décisions aussi fondamentales en terme de libertés individuelles, par le biais de décrets promulgués en catimini, et se soustraire ainsi au débat parlementaire et public nécessaire dans un souci de démocratie (...). L'extension du droit de fichage policier est symptomatique d'une gestion de la sécurité publique malade de ses dérives autoritaires et il est inconcevable pour le « pays des droits de l'homme » - qui a fait de la Liberté le premier mot de sa devise - de prendre un tel virage sécuritaire nous conduisant au péril de la création d'un délit d'opinion et de la surveillance de masse ».

Dans ces conditions, il est proposé à l'Assemblée de Corse qu'elle :

- **REAFFIRME** solennellement son attachement aux libertés publiques et notamment à la liberté d'expression, la liberté syndicale et la liberté d'opinion de conscience et de religion.

⁶ <https://www.interieur.gouv.fr/Actualites/L-actu-du-Ministere/Livre-blanc-de-la-securite-interieure>

- **CONSTATE** que les décrets du 2 décembre 2020 portent gravement atteinte aux dites libertés publiques.
- **DEMANDE** en conséquence au Gouvernement d'abroger ces décrets.
- **APPELLE** à une large mobilisation de tous les démocrates pour obtenir au plus vite ladite abrogation.
- **DONNE MANDAT** au Président du Conseil exécutif de Corse pour agir en justice contre ces textes.

Je vous prie de bien vouloir en délibérer.

Annexe I : Décret n° 2020-1510 du 2 décembre 2020 « fichier ESAP »
(voir fichier PDF joint)

Annexe II : Décret n° 2020-1511 du 2 décembre 2020 « fichier PASP »
(voir fichier PDF joint)

Annexe III : Décret n° 2020-1512 du 2 décembre 2020 « fichier GIPASP »
(voir fichier PDF joint)

Annexe IV : Avis CNIL PSAP
(voir fichier PDF joint)