

La Revue
des Droits
de l'Homme

La Revue des droits de l'homme

Revue du Centre de recherches et d'études sur les
droits fondamentaux

Actualités Droits-Libertés | 2014

Fichage partout, oubli nulle part ? Le Conseil d'Etat ouvre un boulevard au fichier « TAJ »

Droit au respect de la vie privée et protection des données personnelles

Marc Duranton et Jean-Philippe Foegle



Édition électronique

URL : <http://journals.openedition.org/revdh/849>

DOI : 10.4000/revdh.849

ISSN : 2264-119X

Éditeur

Centre de recherches et d'études sur les droits fondamentaux

Référence électronique

Marc Duranton et Jean-Philippe Foegle, « Fichage partout, oubli nulle part ? Le Conseil d'Etat ouvre un boulevard au fichier « TAJ » », *La Revue des droits de l'homme* [En ligne], Actualités Droits-Libertés, mis en ligne le 16 juillet 2014, consulté le 19 avril 2019. URL : <http://journals.openedition.org/revdh/849> ; DOI : 10.4000/revdh.849

Ce document a été généré automatiquement le 19 avril 2019.

Tous droits réservés

Fichage partout, oubli nulle part ? Le Conseil d'Etat ouvre un boulevard au fichier « TAJ »

Droit au respect de la vie privée et protection des données personnelles

Marc Duranton et Jean-Philippe Foegle

1 Traducteur historique d'Edgar Allan Poe, Charles Baudelaire eut l'occasion, au détour de la tribune que lui donnait sa préface aux *Histoires extraordinaires*, de relever que « *parmi l'énumération nombreuse des droits de l'homme que la sagesse du XIXe siècle recommence si souvent et si complaisamment, deux assez importants ont été oubliés, qui sont le droit de se contredire et le droit de s'en aller* ». D'histoires extraordinaires, il ne sera pas ici question. Sauf à considérer bien sûr la collecte de données à caractère personnel (état civil, situation familiale, professionnelle, photographies, entre autres) de millions de personnes, ainsi que leur conservation pendant plusieurs décennies au sein d'un fichier informatique, comme une histoire extraordinaire en soi. Position qui n'est pourtant pas celle du Conseil d'Etat, lequel, dans sa décision n° 360759 du 11 avril 2014, a validé, presque sans réserves, l'arsenal réglementaire qui lui était soumis.

2

3 Etait donc en cause ici un dérivé de ce que Loïc Wacquant aurait pu qualifier de « *panoptisme administratif* »¹. En effet, la loi n° 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure (LOPPSI), assume t'elle, entre autres, l'insertion des articles 230-6 et suivants dans le code de procédure pénale (CPP). L'article 230-6 du CPP précise en ce sens qu'« *afin de faciliter la constatation des infractions à la loi pénale, le rassemblement des preuves de ces infractions et la recherche de leurs auteurs, les services de la police nationale et de la gendarmerie nationale peuvent mettre en œuvre des traitements automatisés de données à caractère personnel recueillies (...) au cours des enquêtes préliminaires ou de flagrance ou des investigations exécutées sur commission rogatoire et concernant tout crime ou délit ainsi que les contraventions de la cinquième classe (...)* ».

4 Ces articles anticipaient alors la fusion des deux fichiers d'antécédents judiciaires utilisés respectivement jusqu'alors par la police et la gendarmerie nationales, à savoir les fichiers

STIC et JUDEX (officiellement disparus en décembre dernier). Et ce, au profit du traitement des antécédents judiciaires (TAJ). Nouvel outil d'investigation des enquêtes pénales et administratives, le TAJ est donc appelé à devenir, de fait, le fichier le plus volumineux (ce dernier intégrant les données contenues au sein des précédents fichiers). Rappelons qu'en décembre 2012, la Commission Nationale Informatique et Libertés (CNIL) estimait que le STIC regroupait 44 millions de procédures, 6,5 millions de personnes mises en cause, et 30 millions de victimes (en 2008, ces chiffres se situaient, toujours selon la Commission, à « seulement » 36 millions de procédures, pour 5,5 millions de personnes mises en cause et 36 millions de victimes).

- 5 Las ! En leurs temps (pas si révolus), les fichiers STIC et JUDEX furent sévèrement et régulièrement critiqués pour leurs nombreux dysfonctionnements, justement par la CNIL, ou encore par la Commission Nationale Consultative des Droits de l'Homme : durées de conservation délirante de données sensibles, techniques différenciés d'enregistrement des infractions, effacement aléatoire des données, accessibilité trop large aux fichiers... Autant de constats qui dénotaient, au mieux, un manque chronique de rigueur, et au pire, la preuve que la vie privée est effectivement un « *problème de vieux cons* », comme le relevait en 2009 le journaliste Jean-Marc Manach.
- 6 **Il n'en demeure pas moins que le TAJ, créé par le décret n° 2012-652 du 4 mai 2012, reprend les principaux traits saillants qui ont fait la renommée de ses deux prédécesseurs.** Ainsi, le décret est venu intégrer les articles R.40-23 et suivants au sein du CPP, lesquels définissent « *les données recueillies (...) qui pourront figurer dans le fichier, ainsi que leur durée de conservation. Il [le décret] liste les personnes ayant accès à ces données et prévoit une procédure de contrôle ainsi qu'un droit d'accès* ». A titre d'exemple, l'article R.40-25 précise les personnes concernées ; l'article R.40-26 liste les informations prises en compte par le fichier ; l'article R.40-27 la durée de conservation des données ; l'article R.40-28 les personnes habilitées à le consulter ; l'article R.40-31 les demandes d'effacement et de rectification, etc.
- 7 Elevé au contentieux par la Ligue des Droits de l'Homme (LDH), le dispositif fut donc validé dans son ensemble par la Haute juridiction, et ce dans la continuité des précédentes solutions jurisprudentielles (et notamment constitutionnelles). Le Conseil d'Etat est également venu préciser que « *les décisions en matière d'effacement ou de rectification prises par le procureur de la République ou par le magistrat [désigné à cet effet], qui ont pour objet la tenue à jour de ce fichier et sont détachables d'une procédure judiciaire, constituent non pas des mesures d'administration judiciaire, mais des actes de gestion administrative du fichier. Elles peuvent, par suite, faire l'objet d'un recours pour excès de pouvoir devant le juge administratif* ».
- 8 L'apport principal de la décision réside donc dans l'ouverture d'un recours à l'encontre des décisions d'effacement ou de rectification, et ce alors même que la loi optait pour un silence retentissant sur ce point précis. Pour autant, ce très relatif « *élément de consolidation juridique* »² peut se révéler surprenant, dans la mesure où **cette possibilité de recours légitime à elle seule, et de manière implicite, non seulement les missions intrusives du fichier, mais encore les larges modalités d'action qui lui sont octroyées.** D'aucuns y verront la négation d'un droit au respect de la vie privée (entendu ici comme droit universel), au profit d'une protection de la vie privée devenue juridictionnelle, c'est à dire examinée au cas par cas.

- 9 A l'heure où le souhait de Baudelaire (timidement ?) se matérialise, force est de constater que le « *droit à l'oubli numérique* » n'a pas encore atteint les abrupts rivages du fichage institutionnel. En ce domaine, le régime du « *dans le doute* » prévaut encore et toujours. L'on peut dès lors se demander si le Conseil d'Etat, à l'instar de Giovanni Drogo dans le *Désert des Tartares*, ne se trompe pas, lui aussi, d'adversaire. Entre « *frénésie sécuritaire* »³ d'une part et protection de la vie privée d'autre part, le sillon est depuis longtemps tout creusé : le contrôle juridictionnel hésite donc peu et opte pour un examen pour le moins élastique (1°). La Haute juridiction décide néanmoins, en dehors de la lettre de la loi, l'ouverture d'un droit au recours contre les refus d'effacement, qui pose avant tout l'enjeu de son effectivité (2°).

1°/- Une protection de la vie privée à prendre au conditionnel

- 10 En d'autres temps et pour d'autres domaines, d'autres lois ont pu être qualifiées de « lois du sauf si ». Pour autant, le vocable conserverait toute sa pertinence dans la décision qui retient ces lignes. Plus généralement, c'est bien de **la conciliation théorique de deux notions cardinales du droit dont il est ici question, à savoir la conciliation entre sécurité et liberté**. Sans revenir sur la frénésie sécuritaire⁴ aujourd'hui à l'œuvre, il semblerait néanmoins que la spécificité de l'accommodement opéré réside dans le fait que celui-ci n'est plus envisagé sous un angle objectif, mais bel et bien subjectif. Ou, pour le dire autrement, ce n'est pas tant les principes véhiculés par le décret litigieux (certainement critiquables en tous points) qui constituent la base du raisonnement auquel le Conseil d'Etat a abouti, mais plutôt leur application concrète, au cas d'espèce (c'est à dire au cas de la personne désireuse d'exercer un recours contre la présence de données la concernant au sein du fichier). De ce point de vue, les quelques barrières dressées à la hâte peuvent apparaître bien fragiles, au regard de ce qu'aurait pu signifier une censure pleine et entière.
- 11 A garder ce sacrifice de la vie privée sur l'autel de la sécurité à l'esprit, la décision du Conseil d'Etat demeure somme toute assez « classique » (bien que brutale), et s'inscrit dans la droite ligne des précédentes solutions jurisprudentielles⁵. Passons sous silence le fait que les moyens liés à la constitutionnalité des dispositions législatives ne pouvaient juridiquement que se voir écartés, notamment en raison du fait que le Conseil constitutionnel a, dans sa décision n° 2011-625 du 10 mars 2011 (ADL du 17 mars 2011) conclu à la conformité à la Constitution des différents articles concernés. Non, plus fondamentalement, le Conseil d'Etat écarta successivement l'ensemble des arguments avancés par la LDH, et, parmi eux, ceux relatifs à l'atteinte à la vie privée, à la durée de conservation excessive des données, et au manque d'encadrement dévolu au fichier.
- 12 Ainsi en est-il donc de l'article R. 40-26 du CPP, qui précise que « *peuvent être enregistrées dans le présent traitement les catégories de données à caractère personnel et informations suivantes : (...) [une] photographie comportant des caractéristiques techniques permettant de recourir à un dispositif de reconnaissance faciale / [d'] autres photographies* ». Après avoir relevé que « *la collecte, la conservation et la consultation de photographies (...) ne portent pas, en elles-mêmes, une atteinte excessive à la protection de la vie privée garantie par l'article 8 de la Convention européenne de sauvegarde des droits de l'Homme et des libertés fondamentales* » (considérant n° 9), le Conseil d'Etat conclut que ladite collecte est, « *compte tenu des*

restrictions et précautions dont est ce traitement est assorti, adéquate, pertinente et non excessive ».

- 13 Deux poids, deux mesures. Rappelons, si cela s'avère nécessaire, que sont ici en jeu des données qualifiées de « sensibles » par les différentes instances internationales⁶, qui ont œuvré en faveur d'une politique législative en la matière : groupe de travail « Article 29 », article 8 de la Charte des Droits Fondamentaux de l'Union Européenne, règlement CE n° 45/2001 relatif au traitement des données... En ce qui la concerne, la CNIL avait par ailleurs relevée, dans sa délibération du 6 juillet 2011, « *que cette fonctionnalité d'identification, voire de localisation, des personnes à partir de l'analyse biométrique de la morphologie de leur visage, présente des risques importants pour les libertés individuelles, notamment dans le contexte actuel de multiplication du nombre des systèmes de vidéoprotection* ». Pour autant, cette position n'a toutefois pas de quoi surprendre : le Conseil d'Etat s'est en effet déjà prononcé en ce sens sur la légalité d'un fichier recueillant des données numérisées, dans le cadre d'un contentieux porté notamment par le GISTI et touchant au recueil de photographies des ressortissants étrangers⁷.
- 14 Deuxième coup de projecteur, les durées de conservation des données collectées, envisagées par l'article R. 40-27 du CPP. Constat préalable, le panel apparaît varié, pour ne pas dire touffu : la durée de conservation de droit commun des données personnelles est fixée vingt ans ; pour autant, ce nombre peut être ramené à cinq ans (cas des infractions routières et de certaines atteintes à la personne) ; élevé à quarante ans (cas des infractions criminelles) ; si elles sont conservées en principe cinq ans, les données concernant les mineurs peuvent, par dérogation, être conservées dix ou même vingt ans ; les données concernant les victimes sont disponibles quinze ans...
- 15 En la matière, le Conseil d'Etat relève que, « *si elles sont supérieures aux délais de prescription de l'action publique, elles [les durées de conservation] trouvent une justification (...) dans la finalité de police judiciaire du traitement (...). Dans ces conditions, et sous réserve de la nécessaire exactitude des données traitées et de leur mise à jour régulière, ces durées n'excèdent pas (...) ce qui est nécessaire (...)* » (considérant n° 13). Encore une fois, l'on retrouve ici une position équivalente à celle présente dans la décision GISTI évoquée⁸. Il n'en demeure pas moins que le silence est éloquent, et ce d'autant plus que la Cour européenne des droits de l'Homme rappelle fréquemment que « *la mémorisation par une autorité publique de données relatives à la vie privée d'un individu constitue une ingérence au sens de l'article 8. L'utilisation ultérieures des informations mémorisées importe peu* »⁹. Pour autant, il serait certainement pertinent de relever que la censure de telles durées de conservation aurait fatalement amené le Conseil d'Etat à préciser, d'un point de vue quantitatif, ce qu'il entendait au travers de la notion de caractère raisonnable des durées de conservation ; quantification qu'il s'est visiblement refusé de proposer.
- 16 Dernier focus, celui axé sur l'autorité principale de contrôle, prévue par l'article 230-8 du CPP et précisée par l'article R. 40-31 de ce même code. L'article 230-8 confie cette mission de contrôle notamment au procureur de la République, lequel peut ordonner que les données soient effacées, complétées ou rectifiées, dans un délai d'un mois à partir de la demande. Ce dernier conserve en outre la faculté de maintenir les informations dans le TAJ, même en cas d'acquiescement ou de relaxe. A noter en outre que toute demande de consultation fait également l'objet d'une mention au sein dudit fichier, et ce pendant cinq ans (article R. 40-30 CPP). Enfin, l'article 230-9 du CPP précise qu'« *un magistrat, (...) désigné à cet effet par le ministre de la justice, concourt à l'application de l'article 230-8 (...). Il a les mêmes pouvoirs que le procureur de la République* ».

- 17 Le Conseil d'Etat ne remet pas en cause le principe énoncé, estimant que « *les décisions prises en matière d'effacement ou de rectification prises par le procureur de la République ou par le magistrat (...) ont pour objet la tenue à jour de ce fichier et sont détachables d'une procédure judiciaire, constituant non pas des mesures d'administration judiciaire, mais des actes de gestion administrative du fichier* » (considérant n° 19). En d'autres termes, la durée de conservation des fichiers est principalement dévolue à une autorité qui n'est pas indépendante aux yeux de la Cour européenne des droits de l'Homme¹⁰. En ce qui concerne les fichiers de police, la CEDH a pu estimer, dans une affaire *S. et Marper c/ Royaume-Uni* du 4 décembre 2008, que « *la Cour est frappée par le caractère général et indifférencié du pouvoir de conservation en vigueur (...). De plus, il n'existe que peu de possibilités pour un individu acquitté d'obtenir l'effacement des données de la base nationale ou la destruction des échantillons ; en particulier, le législateur n'a pas prévu l'exercice d'un contrôle indépendant de la justification de la conservation sur la base de critères précis (...)* ». Plus que jamais donc, **la présence d'un contrôle juridictionnel indépendant apparaît donc comme une réponse à une exigence conventionnelle**, la Cour ayant déjà pu estimer la seule présence du procureur comme insuffisante.
- 18 Au vu de ces trois dispositions sommairement présentées, et des réponses qui y sont successivement apportées, il ressort que tout point de vue qui plaiderait pour un fichage raisonné des personnes, peut difficilement être soutenu. Sous cet angle, le contrôle de proportionnalité traditionnellement invoqué, et qui veut que « *pour être légale, une mesure portant atteinte à une liberté doit être adaptée, nécessaire et proportionnée* »¹¹, apparaît bien peu conciliable avec ce paradigme du « dans le doute » qui règne sans partage au sein du décret attaqué.
- 19 Et ce d'autant plus que, comme cela fut déjà souligné, les irrégularités présentes dans la gestion des fichiers sont connues, les différents rapports évoquant tantôt les risques de fuite, la mise à jour tardive (quand elle n'est pas inexistante) des données... Il est également intéressant de garder à l'esprit le fait que les législations communautaires en la matière, et plus précisément la directive 95/46 CE du 24 octobre 1995¹², ne cessent de rappeler que ces dernières ne doivent être conservées que pendant une durée limitée¹³.

*

- 20 En définitive, l'on ne peut s'empêcher d'imaginer que le raisonnement a été tenu « à l'envers » : certes, les personnes concernées pourront contester les décisions de refus du procureur dans le cadre d'un recours pour excès de pouvoir, mais quel aurait été le besoin d'y recourir si jamais les garanties avaient été suffisantes dans les dispositions mêmes du décret litigieux ? Au reste, d'un point de vue éminemment plus « pratique », ce recours interroge, dans la mesure où « *les difficultés matérielles de la justice judiciaire, aujourd'hui, connues de tous pourraient être un frein au contrôle régulier d'un fichier dont il est déjà avéré qu'il a importé les inexactitudes de ses prédécesseurs* »¹⁴.
- 21 Validant de manière contestable la conservation de données potentiellement sensibles pour des durées importantes, le conseil d'Etat démontre de ce fait, la faiblesse du « triple contrôle » opéré sur les fichiers de police. A l'usage, celui-ci n'apparaît que faiblement protecteur des administrés tant le juge administratif se montre réticent à en tirer l'ensemble des conséquences. Les juges du Palais-Royal semblent toutefois – et c'est là l'apport principal de l'arrêt commenté – avoir pris acte du caractère problématique de

l'absence de recours effectif dont disposeraient les mis en cause pour obtenir l'effacement des données le concernant en cas d'inexactitude de celles-ci.

*

2°/- Une garantie procédurale bien faible dans l'exercice du « droit à l'oubli » dans les fichiers de police

- 22 La loi n° 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure (dite « LOPPSI »), a prévu deux voies pour l'exercice du droit de rectification. La première consiste à s'adresser au procureur de la République territorialement compétent « *sous le contrôle duquel le traitement des données personnelles est opéré* » (Article 230-8 du code de procédure pénale) ; la seconde consiste à s'adresser à un magistrat nommé par le ministre « *chargé de suivre la mise en œuvre et la mise à jour* » du TAJ et disposant à cet égard « *du même pouvoir d'effacement que le procureur de la République* » (Article 230-9 du code de procédure pénale). Si la compétence du procureur de la République n'est pas une nouveauté, celle du magistrat nommé par le ministre en revanche une innovation, issue des conclusions du groupe de contrôle sur les fichiers de police et de gendarmerie (Rapport « Mieux contrôler les fichiers de police », décembre 2008, proposition n° 13).
- 23 La création d'un « magistrat référent » contribue indéniablement à la garantie du droit à la vie privée des administrés en plaçant un peu plus la gestion des fichiers de police sous l'autorité et la garantie du contrôle du pouvoir de l'autorité judiciaire. Pour autant, le législateur ne semble pas s'être préoccupé des voies de recours ouvertes contre les décisions de refus d'effacement émanant du procureur et du magistrat référent, alors que des procédures de rectification ont, au contraire, été ouvertes par la loi dans le cadre d'autres fichiers. Ainsi en est-il du Fichier National Automatisé des Empreintes Génétiques (FNAEG) : pour obtenir la rectification de données du FNAEG, le requérant doit saisir le procureur de la République territorialement compétent (Article R.53-13-1 du CPP). En cas de refus de la part de ce dernier d'autoriser l'effacement, le requérant peut par la suite saisir le juge des libertés et de la détention (Article 53-13-2 du CPP), dont la décision peut être contestée devant le président de la chambre de l'instruction (Article R. 53-13-4 du CPP).
- 24 Le Fichier Judiciaire National Automatisé des Auteurs d'Infractions Sexuelles ou Violentes (FJAISV) prévoit également un dispositif similaire à l'article 706-53-10 du CPP. Se prononçant sur ce fichier, le Conseil Constitutionnel a d'ailleurs considéré que « *l'attribution à l'autorité judiciaire du pouvoir d'inscription et de retrait des données nominatives* » constitue un élément de conciliation proportionnée entre le respect de la vie privée d'une part et la sauvegarde de l'ordre public d'autre part (Conseil Constitutionnel, Décision n° 2004-492 DC du 2 mars 2004 § 87). Cette question du recours effectif – qui rejoint plus largement celle du « droit à l'oubli » en matière de fichage administratif¹⁵ – apparaît d'autant plus pressante qu'une requête pendante devant la Cour Européenne des droits de l'Homme, relève, précisément, la non-conformité des modalités de gestion du fichier « STIC » au regard de l'article 13 de la Convention Européenne des droits de l'homme

(Cour EDH, 5^e Sect., requête n° 21010/10 initiée le 29 mars 2010 par Francois-Xavier BRUNET contre la France et communiquée par la Cour le 14 septembre 2011).

- 25 C'est cette « épée de Damoclès » européenne qui semble avoir déterminé le Conseil d'Etat à mettre en œuvre, par l'ouverture d'un recours pour excès de pouvoir contre les décisions du magistrat référent, une voie de recours supplémentaire contre les refus d'effacement des fichiers de police. La première étape du raisonnement du Conseil d'Etat avait d'ores et déjà été, en réalité, réalisée par une décision du 17 juillet 2013¹⁶. Dans cet arrêt, qui concernait les données nominatives figurant dans le « Système de Traitement des Infractions Constatées », le Conseil d'Etat avait jugé que les décisions en matière d'effacement ou de rectification sont détachables d'une procédure judiciaire et constituent dès lors des actes de gestion administrative du fichier, notamment en raison du fait que les décisions prises par le procureur de la République ne se rapportent qu'à des affaires closes. Celles-ci peuvent donc, dès lors, faire l'objet d'un recours pour excès de pouvoir devant le juge administratif.
- 26 Le Conseil d'Etat fait ici application du principe, estimant que « *les décisions prises en matière d'effacement ou de rectification prises par le procureur de la République ou par le magistrat (...) ont pour objet la tenue à jour de ce fichier et sont détachables d'une procédure judiciaire, constituant non pas des mesures d'administration judiciaire, mais des actes de gestion administrative du fichier* » (considérant n° 19). La solution apparaît d'autant plus logique que les pouvoirs attribués au magistrat référent en matière de rectification, au niveau national, sont exactement les mêmes que ceux attribués aux procureurs de la République au niveau local, aux termes des articles 230-8 et 230-9 du CPP. A ce titre, la solution présente devrait être applicable à l'ensemble des fichiers énumérés par l'article 230-6 du CPP, mais également à l'ensemble des fichiers énumérés à l'article 230-12 du CPP).
- 27 Ce faisant, le Conseil d'Etat contribue, certes, à apporter des garanties juridictionnelles supplémentaires au « droit à l'oubli » dans les fichiers administratifs. Néanmoins, la complexité du système actuel, faisant intervenir à la fois les procureurs de la République territorialement compétents, le « magistrat référent », ainsi que la CNIL, semble bien peu à même d'assurer l'effectivité de ce droit. La CNIL avait d'ailleurs émis le souhait, dans son avis, que « *le rôle de chacun soit précisé, éventuellement par voie de circulaire, afin d'éviter que des décisions contradictoires ne soient prises dans le cas de saisines multiples* », et ceci afin d'alléger une procédure susceptible de décourager d'éventuels requérants (CNIL, Délibération n° 2011-204 du portant avis sur un projet de décret en Conseil d'Etat relatif à la mise en œuvre d'un traitement de données à caractère personnel dénommé « traitement de procédures judiciaires », 7 juillet 2011)

*

**

- 28 Une lecture sommaire de la décision rendue par le conseil d'Etat laissera, sans doute, un goût amer aux défenseurs du droit à la vie privée. Soulignant de manière extrêmement implicite que la durée de conservation des données pourrait poser problème, les juges du palais Royal estiment néanmoins que la nécessaire exactitude des données traitées et leur mise à jour régulière (§ 13) est de nature à assurer la légalité du décret. L'ensemble des dysfonctionnements constatés dans les fichiers « STIC » et « JUDEX » auraient sans doute permis au conseil d'Etat, dans le cadre de son « triple contrôle », de sanctionner des

durées de conservation que l'on serait tentés de qualifier d'excessives. Celui-ci semble toutefois se satisfaire de cette atteinte aux libertés, considérant implicitement que les garanties issues de la loi « LOPPSI » et du recours pour excès de pouvoir sont de nature à assurer une mise à jour régulière des fichiers de police et, partant, une conciliation harmonieuse entre sécurité et liberté.

- 29 Si la décision contribue au mouvement de « juridictionnalisation » de la gestion des fichiers et que la perspective d'une condamnation strasbourgeoise pour violation de l'article 13 semble s'éloigner, peut-on toutefois se satisfaire de ces maigres garanties procédurales ? Au vu de la complexité de la mise en œuvre d'un éventuel « droit à l'effacement » dans les fichiers de police, celles-ci nous semblent, au contraire, bien faibles et les inquiétudes sur le « super-fichier TAJ », bien réelles. Certes, la marge de manœuvre des juges du Palais-Royal était sans doute bien faible en la matière, le Conseil Constitutionnel ayant d'ores et déjà, au préalable, fait primer les impératifs de l'ordre public sur la protection des libertés individuelles en validant l'essentiel de la loi « LOPPSI ». Il n'en reste pas moins que le Conseil d'Etat pose, par cette décision, une nouvelle pierre à l'édifice sécuritaire, contribuant une fois de plus à un la bonne marche d'un mouvement particulièrement préoccupant pour la garantie des libertés individuelles : **celui d'une inversion radicale de la hiérarchie entre sécurité et liberté** (Charlotte Girard, « *La lutte contre le terrorisme. L'hypothèse de la circulation des normes* », 2012, Bruxelles, Bruylant, 332 pages).

*

- 30 Conseil d'Etat, 10^e et 9^e SSR, 11 avril 2014, *Ligue des droits de l'homme*, Req. n ° 360759.

*

Les Lettres « Actualités Droits-Libertés » (ADL) du CREDOF (pour s'y abonner) sont accessibles sur le site de la Revue des Droits de l'Homme (RevDH) – Contact

NOTES

1. Loïc Wacquant, *Les prisons de la misère*, Paris, Raisons d'agir, 1999 ; chapitre « Vers le social-panoptisme ».
2. Gérald Bégranger, « Le contrôle des fichiers de police par les juges », *AJ Pénal*, p. 176.
3. Christine Lazergues, « Le choix de la fuite en avant au nom de la dangerosité : les lois 1, 2, 3, 4, 5, etc. sur la prévention et la répression de la récidive », *RSC 2012*, p. 274.
4. Voir, entre autres : Marc-Antoine Granger, « Existe t'il un droit fondamental à la sécurité ? », *RSC 2009*, p. 273 ; Henri Leclerc, « De la sureté individuelle au droit à la sécurité », *Où en est la sureté personnelle*, colloque organisé par l'Ordre des avocats au Conseil d'Etat le 8 décembre 2005.

5. Au sein de la décision *Association pour la promotion de l'image* (CE 26 octobre 2011, n° 317827), le Conseil d'Etat précise en effet que « (...) qu'il résulte de l'ensemble de ces dispositions que l'ingérence dans l'exercice du droit de toute personne au respect de sa vie privée que constituent la collecte, la conservation et le traitement, par une autorité publique, d'informations personnelles nominatives, ne peut être légalement autorisée que si elle répond à des finalités légitimes et que le choix, la collecte et le traitement des données sont effectués de manière adéquate et proportionnée au regard de ces finalités ».
6. Sur ce point précis, voir Jean-Philippe Foegle, « La CJUE, magicienne européenne du « droit à l'oubli » numérique », *La Revue des droits de l'homme* [En ligne], Actualités Droits-Libertés, mis en ligne le 16 juin 2014.
URL : <http://revdh.revues.org/840>
7. (...) *Le relevé et la mémorisation des empreintes digitales de certains ressortissants étrangers et la possibilité d'un traitement automatisé de ces informations conformément aux garanties prévues par la loi du 6 janvier 1978, justifiés par la protection de l'ordre public et les objectifs d'intérêt général poursuivis par le législateur, ne portent pas d'atteinte excessive à la protection de la vie privée garantie par l'article 8 de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales ; (...) La collecte des images numérisées du visage et des empreintes digitales des ressortissants étrangers, dans les conditions prévues par le décret attaqué, compte tenu des restrictions et précautions dont ce traitement est assorti, est adéquate, pertinente et non excessive par rapport aux finalités légitimes du traitement ainsi institué »* (CE, 7 mai 2012, n°351396).
8. Le Conseil d'Etat s'étant également prononcé, dans cette décision du 7 mai 2012, sur les durées de conservation des données relatives aux arrêtés d'expulsion et aux interdictions du territoire français.
9. Voir en ce sens *Leander c/ Suède*, 26 mars 1987 ; *Kopp c/ Suisse*, 23 mars 1998 ; *Amann c/ Suisse*, 16 février 2000.
10. Voir en ce sens l'arrêt *Medvedyev et autres c/ France* du 29 mars 2010, et notamment les § 117 à 125 ; l'arrêt *Moulin c/ France* du 23 novembre 2010, et notamment les § 56 à 58
11. M. Guyomar, note sous CE, Ass. 26 octobre 2011, *Association pour la promotion de l'image et autres*, n°317827 ; AJDA 2012, p. 35 et suivantes.
12. De son petit nom directive du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation des données.
13. Voir en ce sens Marie-Laure Basilien-Gainche, « Une prohibition européenne claire de la surveillance électronique de masse », *La Revue des droits de l'homme* [En ligne], Actualités Droits-Libertés, mis en ligne le 14 mai 2014. URL : <http://revdh.revues.org/746>
14. Emmanuelle Allain, « Le contrôle *in abstracto* du juge administratif » *AJ Pénal*, p. 145.
15. Nous signalons à ce sujet le lancement récent d'une campagne de la Ligue des Droits de l'Homme sur la question du « fichage institutionnel », qui souligne les risques que présente ce type de fichage pour le citoyen
16. CE, 10e et 9e SSR, 17 juillet 2013, req. n°359417.

RÉSUMÉS

Le décret du 4 mai 2012, pris en application de la loi du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure (LOPPSI), acte la fusion des fichiers informatiques STIC et JUDEX en créant le traitement des antécédents judiciaires (TAJ). Construit sous les auspices de la performance sans cesse accrue et de la mémoire perpétuelle, le dernier « super fichier des données personnelles » a vocation à collecter, accumuler et surtout conserver les « données relatives aux personnes à l'encontre desquelles il existe des indices graves ou concordants rendant vraisemblable qu'elles aient pu participer à la commission de certains crimes, délits ou contraventions de 5ème classe, ainsi qu'aux victimes de ces infractions ». Le 11 avril dernier, à la suite d'un contentieux porté par la Ligue des Droits de l'Homme, le Conseil d'Etat a validé, presque sans réserves, l'arsenal réglementaire qui lui était soumis. Le « droit de tirer le rideau », si tant est qu'il existe, s'en trouve d'autant plus réduit dans ce théâtre où s'amusent en coulisses les données personnelles, et où l'Etat-pénitence demeure seul en scène.

AUTEURS

MARC DURANTON

Etudiant du Master 2 "Droit de l'Homme" de l'Université de Paris Ouest Nanterre La Défense

JEAN-PHILIPPE FOEGLE

Etudiant du Master 2 "Droit de l'Homme" de l'Université de Paris Ouest Nanterre La Défense