Note d'observations[1]

Protection des données et comités sectoriels : avant et après le RGPD

I. LE CONTEXTE

Les administrations détiennent de nombreuses données à caractère personnel sur les citoyens. Pour la plupart, celles-ci sont enregistrées dans des bases de données particulièrement fiables, appelées des « sources authentiques de données ». Chaque source authentique de données est placée sous la responsabilité de l'administration qui la détient, qui est chargée de vérifier l'exactitude des données et d'en assurer la mise à jour[2].

Depuis une réforme législative intervenue en 2003, et jusqu'à l'entrée en vigueur du RGPD le 25 mai 2018, l'accès aux données contenues dans ces sources authentiques de données était conditionné à l'obligation d'obtenir l'autorisation du comité sectoriel compétent[3]. Parmi les comités sectoriels existants figurait le Comité sectoriel Autorité fédérale, compétent pour autoriser l'accès aux sources authentiques de données détenues par un Service public fédéral ou par un organisme public doté de la personnalité juridique qui relève de l'autorité fédérale. C'est pourquoi l'accès au registre de la DIV, dont il est question dans l'arrêt commenté, était conditionné à l'obtention d'une autorisation du Comité sectoriel Autorité fédérale, conformément à l'article 36*bis* de la loi du 8 décembre 1992, entré en vigueur le 26 juin 2003 et abrogé suite à l'entrée en application du RGPD le 25 mai 2018.

Les services de police étaient-ils eux aussi contraints de demander pareille autorisation ? Une insécurité juridique existait. D'une part, un arrêté royal du 4 juin 2003[4] dispensait les services de police de l'autorisation imposée par l'article 36*bis* de la loi du 8 décembre 1992. D'autre part, la loi du 19 mai 2010 portant création de la Banque-Carrefour des véhicules leur imposait pareille autorisation. À cet imbroglio normatif s'était encore ajouté un arrêt de la Cour de cassation du 13 décembre 2016, confortant l'obligation pour les services de police de demander une autorisation préalable au Comité sectoriel Autorité fédérale avant d'accéder aux données à caractère personnel des automobilistes.

Pour mettre fin à cette insécurité juridique, le législateur décida d'intervenir par une loi du 14 juin 2017[5]. L'article 2 de cette loi complétait l'article 36*bis* de la loi du 8 décembre 1992 en organisant une « dispense explicite et générale de l'obligation d'autorisation pour les services de police »[6] lorsqu'ils accèdent à des données à caractère personnel provenant d'autres services publics fédéraux. L'article 3 de la loi du 14 juin 2017 ajoutait que cette dispense

1 Elise Degrave. Chargée de cours à la Faculté de droit. Chercheuse au Crids et à la Chaire Egov de l'UNamur.

2 Pour plus d'informations à ce sujet, voy. E. Degrave, *L'e-gouvernement et la protection de la vie privée. Légalité, transparence et contrôle,* coll. Crids, Bruxelles, Larcier, 2014, nos 12 et s.

3 Pour plus d'informations à ce sujet, voy. *ibidem,* nos 534 et s.

4 A.R. du 4 juin 2003 « fixant dérogation à l'autorisation visée à l'article 36*bis* de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel au profit de la banque de données nationale générale de la police intégrée à deux niveaux ».

5 Loi du 14 juin 2017 modifiant l'article 36*bis* de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, *M.B.*, 28 juillet 2017.

6 Extrait des travaux préparatoires de la loi du 14 juin 2017 cité par la Cour dans l'arrêt commenté, B.4.

prenait cours le 26 juin 2003, c'est-à-dire à la date de l'entrée en vigueur de l'article 36*bis* de la loi du 8 décembre 1992[7].

Les articles 2 et 3 de la loi du 14 juin 2017 furent attaqués par deux automobilistes poursuivis pour infraction au Code de la route après que la police les ait identifiés en accédant à leurs données à caractère personnel détenues dans le registre de la DIV.

II. LES QUESTIONS TRANCHÉES PAR LA COUR CONSTITUTIONNELLE

Le recours en annulation introduit par les deux automobilistes amène la Cour à trancher deux questions.

A. L'article 2 de la loi du 14 juin 2017 viole-t-il l'article 22 de la Constitution ?

En d'autres termes, le législateur pouvait-il, par l'article 2 de la loi du 14 juin 2017, dispenser la police de demander l'autorisation du Comité sectoriel Autorité fédérale sans violer l'article 22 de la Constitution qui consacre le droit fondamental à la protection de la vie privée, lu en combinaison avec les articles 7 et 8 de la Charte des droits fondamentaux et l'article 8 de la C.E.D.H. ? En particulier, si les services de police sont dispensés d'obtenir l'autorisation du Comité sectoriel Autorité fédérale, existe-t-il des garanties législatives suffisantes pour encadrer les traitements de données à caractère personnel effectués par ces services ?

La Cour répond par l'affirmative. Elle constate que les traitements de données à caractère personnel effectués par les services de police sont encadrés strictement par la loi du 5 août 1992 sur la fonction de police. Parmi les éléments relevés par la Cour figure le fait que cette loi limite le traitement des données par les services de police aux données adéquates, pertinentes et non excessives au regard des finalités de police administrative et de police judiciaire poursuivies[8]. De plus, ladite loi encadre spécifiquement le traitement, par les services de police, des données obtenues auprès d'un service public fédéral ou d'un organisme fédéral. Par ailleurs, la loi du 5 août 1992 encadre également d'autres éléments essentiels des traitements de données, tels que les catégories de banques de données policières opérationnelles, la nature des données qui peuvent être traitées dans ces banques de données, etc.[9]. La Cour constate également qu'un « Organe de contrôle de l'information policière » a été créé auprès de la Commission de la protection de la vie privée (remplacée depuis lors par l'Autorité de protection des données)[10].

Compte tenu de ces éléments, la Cour affirme que « le législateur a pu estimer qu'il existait des garanties législatives suffisantes pour prévenir les abus en ce qui concerne les traitements de données à caractère personnel par les services de police. Pour cette raison, il a pu également estimer que les services de police pouvaient être dispensés de toute "autorisation préalable de comité sectoriel" »[11].

B. L'article 3 de la loi du 14 juin 2017 viole-t-il l'article 12, alinéa 2, de la Constitution ?

En d'autres termes, le législateur pouvait-il faire rétroagir la dispense des services de police d'obtenir l'autorisation du Comité sectoriel Autorité fédérale au 25 juin 2003, soit à la date de l'entrée en vigueur de l'article 36*bis* de la loi du 8 décembre 1992 ? En agissant ainsi, le législateur a-t-il respecté l'article 12, alinéa 2, de la Constitution, qui organise le principe de légalité et de prévisibilité en matière pénale ?

La Cour répond par la négative. Selon elle, l'article 12, alinéa 2, de la Constitution est appli-

7 Arrêt commenté, B.1 et B.4.

8 Arrêt commenté, B.12.1.

9 Arrêt commenté, B.12.3.

10 Arrêt commenté, B.12.4.

11 Arrêt commenté, B.13.

cable en l'espèce, puisqu'il s'applique également aux poursuites pénales.

La Cour rappelle que « l'exigence de prévisibilité de la procédure pénale garantit à tout justiciable qu'il ne peut faire l'objet d'une information, d'une instruction et de poursuites que selon une procédure dont il peut prendre connaissance avant sa mise en œuvre »[12]. « Cette exigence garantit au justiciable que les règles relatives à la démonstration d'une faute d'une personne que doivent respecter les services de police et les instances poursuivantes ne peuvent en principe pas être modifiées rétroactivement au détriment d'une personne »[13].

Et de constater qu'« en conférant un effet rétroactif à la dispense » d'autorisation de comité sectoriel, organisée pour les services de police, la disposition attaquée prive le justiciable « de la garantie que les règles relatives à la démonstration de la faute d'une personne que doivent respecter les services de police et les instances poursuivantes ne peuvent être modifiées rétroactivement au détriment de cette personne »[14].

La Cour annule donc l'article 3 de la loi du 14 juin 2017.

Dès lors, au terme de ce recours, seule la rétroactivité de la dispense d'autorisation – et non la dispense elle-même – est annulée. La Cour constate qu'en principe, la dispense ne peut donc valoir qu'à partir de l'entrée en vigueur de la loi du 14 juin 2017 qui organise cette dispense, c'est-à-dire à partir du 7 août 2017. Cela signifie que, en principe, les traitements de données effectués par les services de police entre le 26 juin 2003 et le 6 août 2017 sont illégaux et qu'il faudrait annuler les poursuites pénales qui se fondent sur ces traitements. Mais, ce faisant, les inconvénients créés par la rétroactivité de l'annulation risqueraient d'être disproportionnés par rapport aux avantages de celle-ci. C'est pourquoi la Cour décide de maintenir les effets de la disposition annulée, « afin d'éviter que les éléments de preuve fondés sur des données à caractère personnel que les services de police ont obtenus avant le 7 août 2017 soient remis en cause »[15]. Il s'agit là d'une technique à laquelle peut recourir la Cour en vertu de la loi spéciale du 6 janvier 1989 sur la Cour constitutionnelle[16], pour que « les conséquences de cette rétroactivité soient corrigées, voire annihilées, et ce à l'égard des effets de la norme annulée »[17].

III. ET MAINTENANT ?

A. La portée de l'arrêt en pratique

Ainsi donc, par cet arrêt, la Cour clarifie la question technique de savoir si, entre le 26 juin 2003 (date de l'entrée en vigueur de l'article 36*bis* de la loi du 8 décembre 1992) et le 24 mai 2018 (veille de l'entrée en application du RGPD qui conduit à l'abrogation de la loi du 8 décembre 1992), les services de police pouvaient accéder aux données à caractère personnel des automobilistes détenues dans le registre de la DIV, sans avoir obtenu au préalable l'autorisation du Comité sectoriel Autorité fédérale. La Cour affirme qu'un tel accès sans autorisation n'était possible qu'entre le 7 août 2017 (date de l'entrée en vigueur de la loi du 14 juin 2017) et le 24 mai 2018, mais elle décide de maintenir les effets de la disposition annulée pour ne pas remettre en cause les procédures opérées entre le 26 juin 2003 et le 24 mai 2018.

La portée de cet arrêt ne se réduit toutefois pas à la résolution de cette question limitée dans le temps. Les développements de la Cour ont le mérite de mettre en exergue l'importance de

12 Arrêt commenté, B.24.3.
13 Arrêt commenté, B.24.4.
14 Arrêt commenté, B.26.
15 Arrêt commenté, B.28.
16 Article 8 de ladite loi.
17 M. Verdussen, *Justice constitutionnelle,* Bruxelles, Larcier, 2012, p. 270.

baliser, au niveau législatif, le traitement des données à caractère personnel des citoyens qui sont détenues par l'État. Le droit à la protection de la vie privée, consacré notamment par l'article 22 de la Constitution, n'est pas un droit absolu. Il est possible d'organiser des ingérences dans ce droit, telles que des traitements de données à caractère personnel, à condition que les éléments essentiels de ces traitements fassent l'objet de garanties législatives claires[18]. C'est d'autant plus important que, s'agissant des données détenues par l'État, le consentement de la personne concernée ne joue en principe pas. En effet, dans ses relations avec l'État, chacun est, en principe, obligé de fournir ses informations personnelles. S'il refuse d'être enregistré au Registre national, il n'aura pas d'existence civique. S'il refuse de communiquer ses données fiscales, cadastrales, sociales, etc., il ne remplit pas ses obligations civiques et encourt de lourdes sanctions. Les règles qui encadrent les traitements de ces données doivent donc être fixées par le législateur, au terme d'un débat démocratique, et rédigées de manière claire et compréhensible.

Par ailleurs, l'arrêt commenté met également en évidence que cette exigence de légalité et de prévisibilité de loi encadrant un traitement de données à caractère personnel est d'autant plus forte lorsque des données à caractère personnel sont utilisées dans le cadre d'une procédure pénale. En effet, les règles qui encadrent l'utilisation de telles données doivent alors non seulement respecter l'exigence de légalité et de prévisibilité découlant de l'article 22 de la Constitution, mais également respecter les garanties qui découlent de l'article 12 de la Constitution, qui consacre le principe de légalité et de prévisibilité en matière pénale. C'est d'ailleurs sur la base de ce principe que la Cour a annulé la rétroactivité de la dispense d'autorisation organisée pour les services de police.

B. La suppression des comités sectoriels et leur remplacement par des protocoles

L'arrêt commenté éclaire également la question de savoir dans quelles hypothèses une autorisation de comité sectoriel est nécessaire. Néanmoins, cette question n'a plus lieu d'être désormais. À l'occasion de la mise en place de l'Autorité de protection des données qui remplace désormais la Commission de la protection de la vie privée, les comités sectoriels ont été supprimés[19].

La suppression des comités sectoriels et, par là, la disparition du contrôle qu'ils effectuaient sur les traitements de données, pose question. Ainsi qu'on l'a évoqué à l'entame de cette contribution, les comités sectoriels étaient des organes institués au sein de la Commission de la protection de la vie privée pour autoriser, ou refuser, le transfert des données détenues par l'État. Chaque source authentique de données était protégée par un comité sectoriel spécifique. Ainsi, le comité sectoriel Registre national contrôlait l'usage fait des données enregistrées dans la source authentique « Registre national »[20], le comité sectoriel de la sécurité sociale et de la santé contrôlait les données enregistrées dans les sources authentiques des administrations œuvrant en matière de sécurité sociale et de santé[21], le comité sectoriel de

18 Cour eur. D.H., arrêt *Rotaru c. Roumanie*, 4 mai 2000, req. n° 28341/95, § 57, *R.T.D.H.*, 2001, pp. 137 et s., note O. De Schutter ; Cour eur. D.H., arrêt *Shimovolos v. Russia,* 21 juin 2011, req. n° 30194/09, § 69 ; E. Degrave, *L'e-gouvernement et la protection de la vie privée. Légalité, transparence et contrôle, op. cit.*, n^os^ 102 et s.

19 Voy. l'article 109 de la loi du 3 décembre 2017 portant création de l'Autorité de protection des données.

20 Article 5 de la loi du 8 août 1983 organisant un registre national des personnes physiques ; arrêté royal du 17 décembre 2003 fixant les modalités relatives à la composition et au fonctionnement de certains comités sectoriels institués au sein de la Commission de la protection de la vie privée.

21 Articles 37 à 52 de la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque-Carrefour de la sécurité sociale.

la Banque-Carrefour des entreprises contrôlait les données de la Banque-Carrefour des entreprises[22], etc. Certes, ces comités sectoriels n'étaient pas à l'abri de toute critique, notamment en ce que leur indépendance n'était pas garantie[23]. Mais ils avaient le mérite de jouer le rôle de « chien de garde » des sources de données authentiques détenues par l'État, en agissant, en principe, de manière cohérente avec les avis et les positions de la Commission vie privée. En d'autres termes, face à l'incapacité du législateur et du Gouvernement d'anticiper la multitude des traitements de données au sein de l'administration, les comités sectoriels constituaient un relais qui sur le terrain veillait, en principe, au respect des normes, au cas par cas. En outre, les décisions des comités sectoriels étaient publiques et accessibles en ligne via le site internet de la Commission de la protection de la vie privée.

Au moment de l'adoption de la loi du 3 décembre 2017 qui a institué l'Autorité de protection des données et supprimé les comités sectoriels, le législateur lui-même ignorait encore par quoi ces comités sectoriels allaient être remplacés. Il s'avère à présent que ce contrôle a été remplacé par des mesures parcellaires, sans cohérence et dont la transparence laisse perplexe.

Pour l'essentiel, et en principe, le contrôle des comités sectoriels est remplacé par la rédaction de protocoles entre administrations. Ces protocoles sont visés à l'article 20 de la loi du 30 juillet 2018[24]. En somme, lorsque des données provenant d'une autorité publique fédérale sont communiquées à une administration, un protocole doit être rédigé par les deux autorités impliquées dans cet échange. Par exemple, lorsqu'une commune demande la communication de données détenues par l'Administration générale de la documentation patrimoniale – qui fait partie du SPF Finances – en vue d'octroyer les permis d'urbanisme, un protocole devra être rédigé avant que cette autorité publique fédérale transfère les données demandées.

Ce protocole est obligatoire, mais des exceptions peuvent être prévues par la loi. Notons qu'il ressort des travaux préparatoires de cette loi[25] qu'un tel protocole ne doit pas être rédigé pour les flux internes à la police intégrée au sens de l'article 2, 2°, de la loi du 7 décembre 1998, sans toutefois que cette exception soit explicitement affirmée dans ladite loi.

Malheureusement, selon nous, le système des protocoles est organisé de manière trop laxiste pour constituer une réelle protection des données à caractère personnel issues des sources authentiques de données de l'État. En l'occurrence, on doit s'inquiéter que les échanges de données provenant des sources authentiques de l'État ne soient pas plus protégés.

Tout d'abord, la loi du 30 juillet 2018 n'impose pas les mentions qui doivent figurer dans ces protocoles. Les auteurs du protocole peuvent donc décider de ce qu'ils insèrent dans ledit document, au risque que celui-ci ne détermine pas à suffisance les éléments qui composent le traitement de données organisé.

De plus, non seulement il n'y a plus de contrôle des comités sectoriels mais, de surcroît, ces protocoles ne sont soumis à aucun contrôle

22 Articles 27 à 32 de la loi du 16 janvier 2003 portant création d'une Banque-Carrefour des entreprises (…); arrêté royal du 17 décembre 2003 fixant les modalités relatives à la composition et au fonctionnement de certains comités sectoriels institués au sein de la Commission de la protection de la vie privée.

23 À ce sujet, voy. E. Degrave, *L'e-gouvernement et la protection de la vie privée, op. cit.*, n^os^ 492 et s.

24 Loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel.

25 Exposé des motifs du projet de loi relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, *Doc. parl.*, Ch. repr., session 2017-2018, Doc. 54 3126/001, p. 44.

de l'Autorité de protection des données, ni en amont de la rédaction du protocole, ni en aval.

La nature de ces protocoles, et dès lors les recours dont ceux-ci pourraient faire l'objet, ne sont pas non plus définis.

Dans la foulée, vu le peu de balises légales imposées pour ces traitements de données, on peut craindre qu'en pratique, des chantages émergent entre responsables de traitement, qui consisteraient à conditionner l'envoi de telles données à la réception de telles autres. Il en va d'autant plus ainsi que l'hypothèse où les responsables de traitement ne s'entendraient pas sur les conditions du protocole n'est absolument pas abordée par la loi. On peut ainsi craindre un retour à des pratiques illégales que l'on a connues avant la mise en place de comités sectoriels où, à défaut de procédure claire, il arrivait que des agents de l'administration s'accordent entre eux sur l'envoi de certaines données qui étaient ensuite envoyées par mail non sécurisé. De tels transferts se faisaient en toute opacité, faisant fi de tout examen juridique. De simples protocoles non contrôlés par l'APD ne risquent-ils pas de recréer pareilles dérives ?

Ajoutons à cela que les échanges de données entre administrations risquent désormais de pâtir d'un manque de transparence. Les décisions des comités sectoriels devaient être publiées sur le site internet de la Commission de la protection de la vie privée. Cela permettait de regrouper ces décisions en un point central auquel tout un chacun pouvait avoir aisément accès. Il n'en va malheureusement pas de même pour les protocoles. Ceux-ci doivent être publiés sur le site internet de chaque responsable du traitement concerné par le transfert de données.

Initialement, le gouvernement n'avait d'ailleurs prévu aucune mesure de publicité, ce qui a fait réagir la Section de législation du Conseil d'État[26] et la Commission de la protection de la vie privée[27]. Suite à leurs remarques, le gouvernement a ajouté à la disposition concernée que le protocole serait publié sur le site internet des responsables de traitement concernés.

Nous déplorons cette solution. Compte tenu du nombre d'institutions concernées, de la qualité très variable de leur site internet dont certains ne sont pas à jour ou particulièrement fastidieux à lire, on doute fort que pareille mesure aide tout qui le souhaite à prendre connaissance et comprendre sans trop de difficultés les traitements de données opérés par les autorités publiques fédérales. Il aurait été bien plus judicieux de centraliser pareille publicité sur le site internet de l'Autorité de protection des données en les classant selon un critère clair qui pourrait être lié au type de données traitées.

Enfin, comme on l'a dit, la rédaction de protocoles est le contrôle de principe, mais non le modèle unique de contrôle. Pour certains types de données issues du secteur public, le législateur a opté pour un mécanisme de contrôle différent. Cela ne favorise pas non plus la lisibilité et la compréhension de la matière. Ainsi, les données du Registre national, les données de sécurité sociale et de santé font l'objet d'un contrôle particulier, qui n'est pas à l'abri de critiques lui non plus[28].

Il reste à espérer que l'Autorité de protection des données portera toute l'attention et l'énergie nécessaires au contrôle des traitements de données effectués par les institutions

[26] SLCE, avis n° 63.192/2 du 19 avril 2018, *op. cit.*, Doc. 54-3126/001, p. 424.

[27] CPVP, avis n° 33/2018 du 11 avril 2018 sur un avant-projet de loi «relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel», *Doc. parl.*, Ch. repr., 2017-2018, Doc. 54-3126/001, pp. 782-783, n° 162.

[28] Pour plus d'informations à ce sujet, voy. E. Degrave et C. de Terwangne (avec la collaboration de A. Delforge et L. Gérard), *Le RGPD et les lois belges,* Bruxelles, Politeia, 2019, à paraître.

publiques. C'est d'autant plus important que, dans le contexte actuel, il est devenu très difficile, pour tout un chacun, de prendre connaissance de ces traitements et d'en dénoncer les abus. Le travail de l'Autorité de protection des données, agissant dans l'intérêt général des citoyens, sera donc essentiel.

Elise Degrave