LE CONSEIL CONSTITUTIONNEL
ET LA PROTECTION DES DONNÉES PERSONNELLES

Corinne Luquiens

Membre du Conseil constitutionnel français

Après la présentation faite ce matin par Michel Pinault sur le thème de la fin de vie, je vais, cet après-midi, évoquer la récente jurisprudence du Conseil constitutionnel sur la question de la protection des données en présentant les grandes lignes de notre décision n° 2018-765 DC du 12 juin 2018 sur la loi relative à la protection des données personnelles.

Nous avons, en effet, été saisis, dans le cadre du contrôle a priori, par plus de soixante sénateurs, de ce texte transposant dans notre droit interne ce qu'il est d'usage d'appeler « le paquet européen de protection des données ». Il s'agit des deux textes adoptés le 27 avril 2016 : un règlement 2016/ 679 relatif à la protection des personnes physiques à l'égard des données à caractère personnel (RGDP), directement applicable dans les Etats membres depuis le 25 mai 2018, et une directive 2016/ 680 relative au traitement mis en œuvre à des fins de détection des infractions pénales, d'enquête et de poursuite en la matière ou d'exécution de sanctions pénales qui devait être transposée au plus tard le 6 mai 2018.

Ces deux textes ont pour ambition de tirer les conséquences des nouvelles pratiques numériques et d'harmoniser les normes applicables au niveau européen afin d'assurer une concurrence loyale entre les entreprises européennes, mais aussi, grâce à l'extraterritorialité, de les protéger face à la concurrence d'entreprises étrangères à l'Union. Le périmètre de la législation européenne est en effet étendu aux entreprises qui, sans être établies sur le territoire de l'Union européenne, y collectent et traitent des données relatives à des personnes qui s'y trouvent.

Le choix a été fait, s'agissant de l'utilisation des données personnelles, de passer d'un régime d'autorisation préalable à un régime de responsabilisation des acteurs et, parallèlement, à un élargissement des pouvoirs donnés aux autorités de contrôle.

I. La nature du contrôle du Conseil constitutionnel sur les lois intégrant la réglementation européenne à notre droit interne

Le recours dont nous avons été saisi soulevait d'abord un problème que j'évoquerai rapidement concernant la nature du contrôle qu'exerce le Conseil constitutionnel sur les lois qui intègrent la réglementation européenne à notre droit interne.

S'agissant des directives, notre jurisprudence est maintenant solidement établie. Lorsque la loi nationale se borne à transposer les dispositions précises et inconditionnelles d'une directive, le Conseil ne s'estime pas compétent pour juger de leur conformité à la Constitution, puisque cela reviendrait à se prononcer sur la directive elle-même, sous la réserve cependant qu'aucun principe inhérent à l'identité constitutionnelle de la France ne soit mis en cause.

Nous n'exerçons donc, en la matière, qu'un contrôle restreint, de même que nous ne sanctionnons la loi, en application de l'article 88-1 de la Constitution qui affirme notre participation à l'Union européenne, que si ses dispositions sont manifestement incompatibles avec celles de la directive. Il s'agit, en effet, d'un contrôle qui relèverait normalement de la Cour de justice de l'Union européenne (CJUE) mais le délai d'un mois qui s'impose au Conseil dans le cadre du contrôle a priori ne nous permet pas de la saisir d'une question préjudicielle. C'est donc aux juridictions de fond qu'il incombe, le cas échéant, de le faire ultérieurement à l'occasion d'un litige dont elles seraient saisies.

En revanche, notre contrôle s'exerce dans sa plénitude lorsque la directive laisse au législateur national une marge de manœuvre puisque la loi n'est plus liée par la nécessité de transposer la directive.

Quant aux règlements, ils sont d'application directe et le rôle du législateur se limite donc à mettre la loi nationale en conformité avec leurs dispositions. La décision relative à la protection des données nous a donné l'occasion de préciser que, comme en matière de transposition de directives, nous n'exerçons qu'un contrôle restreint pour nous assurer qu'une disposition législative n'est pas manifestement incompatible avec celle d'un règlement.

Puisque le règlement général sur la protection des données présentait cette particularité de laisser sur de nombreux points, une marge de manœuvre aux Etats membres, le législateur retrouvait dans ces domaines la totalité de ses compétences et, corrélativement, nous avons également exercé dans ces domaines notre contrôle de manière plénière.

II. Le contenu de notre décision sur le fond

J'en viens maintenant au fond de notre décision. Nous avons été saisis par les sénateurs de 11 articles de la loi. Néanmoins, dans le temps limité qui m'est imparti, je n'évoquerai que les sujets majeurs dont nous avons eu à traiter et qui marquent la position du Conseil constitutionnel sur quelques questions relatives à la protection des données personnelles.

1. Pouvoirs de contrôle et de sanction

Nous avons d'abord eu à nous prononcer sur les pouvoirs de contrôle et de sanction de la commission nationale de l'informatique et des libertés (CNIL) qui, depuis la loi du 6 janvier 1978, est, en France, chargée d'encadrer le développement de l'informatique afin de protéger la liberté des citoyens.

a) Le principe d'indépendance et d'impartialité du pouvoir de sanction

La CNIL étant l'autorité chargée de prononcer des sanctions en cas de violation des règles définies par la directive, le règlement et la loi de transposition de ces textes européens, les requérants contestaient d'abord les dispositions de la loi au regard du principe d'indépendance et d'impartialité dans l'exercice des pouvoirs de sanction.

Selon une jurisprudence bien établie, le Conseil juge que les exigences d'impartialité résultant de l'article 16 du la Déclaration des droits de l'homme et du citoyen de 1789 impose une séparation au moins fonctionnelle, sinon organique, entre les fonctions de poursuite et d'instruction, d'une part, et les fonctions de jugement, d'autre part au sein d'autorités administratives disposant d'un pouvoir de sanction.

Depuis quelques années, la CNIL a mis en place une formation restreinte chargée de prononcer d'éventuelles sanctions dont les membres ne participent pas aux fonctions de poursuite et d'instruction. Mais les requérants faisaient d'abord valoir que les agents de la CNIL sont placés sous l'autorité du Président même lorsqu'ils exercent leur activité auprès de la formation restreinte chargée des sanctions. Ils ajoutaient que les membres de cette formation restreinte restaient en contact avec les autres membres de la commission.

En l'occurrence, nous avons cependant constaté que seuls les agents de la CNIL chargés de la tenue des séances, qui ne prennent évidemment pas part à ses décisions, peuvent être présents au cours des délibérés de sa formation restreinte, de sorte que le fait qu'ils soient placés sous l'autorité du Président n'est pas constitutif d'une méconnaissance du principe d'impartialité.

Par ailleurs, nous avons également relevé que les dispositions relatives à la séparation au sein de la CNIL des fonctions de poursuite et d'instruction, d'une part, et des fonctions de jugement et de sanction, d'autre part, n'étaient nullement remises en cause.

b) Le principe de séparation des pouvoirs

Les requérants soutenaient, en outre, que la loi méconnaissait le principe d'autonomie des pouvoirs constitutionnels, qui résulte de la séparation des pouvoirs protégée par l'article 16 de la Déclaration de 1789, en ne prévoyant pas au profit des pouvoirs constitutionnels, sauf l'exercice de leur fonction juridictionnelle par les juridictions, d'exception aux pouvoirs de contrôle de la commission.

Le Conseil a écarté ce grief en constatant que les opérations de contrôle de la CNIL ne sauraient remettre en cause le fonctionnement des pouvoirs publics. Sans que cela soit expressément précisé dans notre décision, il va de soi que les pouvoirs de contrôle de la CNIL ne sauraient interférer avec les prérogatives personnelles du Président de la République ou le fonctionnement des assemblées s'agissant de leur activité

strictement parlementaire. Mais on ne peut l'écarter pour leur activité purement administrative et, moins encore pour l'administration en général, même si celle-ci est placée sous l'autorité du Gouvernement.

2. Traitement de données personnelles en matière pénale

La loi que le Conseil a eu à examiner comporte deux séries de dispositions relatives aux données personnelles en matière pénale : celles, d'une part, relevant du champ de la directive du 27 avril 2016 qui sont traitées par les autorités compétentes, principalement les autorités judiciaires et de police, à des fins de prévention et de détection des infractions pénales, d'enquête et de poursuites en la matière ou d'exécution de sanctions pénales ; celles, d'autre part, auxquelles s'applique le Règlement, collectées par d'autres organismes, par exemple les établissements financiers, qui recueillent et conservent des données personnelles, pour respecter une obligation légale, à des fins de détection et de poursuites d'infractions pénales, les données n'étant transmises aux autorités compétentes que dans les cas prévus par la loi de chaque Etat membre.

Sur ce dernier type de données, le règlement laisse au législateur national des marges de manœuvre, ce qui nous a permis d'exercer un contrôle plénier.

L'article 10 du RGDP prévoit que : « Le traitement des données à caractère personnel relative aux condamnations pénales et aux infractions pénales ou aux infractions ou aux mesures de sécurité connexes… ne peut être effectué que sous le contrôle de l'autorité publique, ou si le traitement est autorisé par le droit de l'Union ou par le droit d'un Etat membre qui prévoit des garanties appropriées pour les droits et libertés des personnes concernées ». La loi de transposition s'est limitée à reprendre les termes du Règlement en prévoyant que les traitements de données à caractère personnel relatives aux condamnations pénales, aux infractions et aux mesures de sûreté connexes ne peuvent être effectués que sous le contrôle de l'autorité publique.

Dans une décision précédente – n° 2004-499 DC – le Conseil avait jugé que les garanties appropriées et spécifiques, justifiées par l'ampleur et la nature des informations traitées, devaient être fixées par la loi et que la définition des exceptions selon lesquelles seule l'autorité publique peut mettre en œuvre de tels traitements ne pouvaient être renvoyée à l'autorité de régulation (la CNIL) ou à des lois ultérieures.

Or, on ne pouvait que constater que le législateur s'était contenté de reprendre les termes du Règlement pour affirmer que les traitements de données ne peuvent être effectués que sous le contrôle de l'autorité publique, sans déterminer les catégories de personnes susceptibles d'intervenir, ni préciser les finalités qui devaient être poursuivies par la mise en œuvre de tels traitements. Eu égard à l'ampleur que peuvent revêtir de tels traitements et à la nature des informations traitées, le Conseil a considéré que les dispositions contestées mettaient en cause les garanties fondamentales accordées aux citoyens pour l'exercice des libertés publiques et, en cohérence avec sa jurisprudence antérieure, les a censurées pour incompétence négative du législateur.

3. Décisions prises sur le fondement d'algorithmes

Le dernier point que je voudrais évoquer n'est pas le moindre puisqu'il s'agit de l'usage des algorithmes pour la prise de décisions administratives. Substituer un traitement automatisé à un examen personnalisé de dossiers est évidemment un sujet sensible. Sans doute l'utilisation d'un algorithme facilite t il, pour les cas complexes et l'examen d'un nombre important de dossiers, une prise de décision administrative rapide et objective, susceptible de mettre les usagers à l'abri de décisions arbitraires. Mais il importe de vérifier que les critères retenus sont satisfaisants et de mettre en place des garanties de procédure et de transparence.

Le RGDP fixe les règles qui s'imposent pour qu'une décision administrative puisse être fondée exclusivement sur un traitement automatisé. Il affirme d'abord le principe selon lequel toute personne peut s'opposer à une décision de cette nature qui produirait des effets juridiques à son égard ou l'affecterait de manière significative.

Ce principe souffre cependant d'exception lorsque la décision est nécessaire à la conclusion ou à l'exécution d'un contrat entre la personne et le responsable du traitement ou lorsqu'elle est autorisée par le droit de l'Union ou de l'Etat membre auquel le responsable du traitement est soumis.

Le Règlement offre une marge de manœuvre au droit national pour autoriser une prise de décision automatisée à condition de prévoir des mesures appropriées pour la sauvegarde des droits et libertés et des intérêts légitimes de la personne concernée.

En tout état de cause, le RGDP écarte la prise de décision automatisée lorsque le traitement est fondé sur des données sensibles, c'est-à-dire les données biométriques, génétiques, de santé, relatives à la vie sexuelle, à la religion ou aux convictions philosophiques.

On relèvera d'abord que jusqu'alors, le droit français excluait que certaines décisions puissent être prises sur le fondement d'un algorithme. Il prévoyait d'abord une interdiction absolue de traitements destinés à évaluer certains éléments de la personnalité pour les décisions de justice impliquant une appréciation sur le comportement d'une personne. Il écartait également le recours exclusif à un algorithme pour les décisions produisant des effets juridiques lorsque le traitement automatisé de données est destiné à définir le profil de l'intéressé ou à évaluer certains aspects de sa personnalité tout en prévoyant des exceptions à cette interdiction pour les décisions prises dans le cadre de la conclusion d'un contrat et pour lesquelles les personnes concernées ont pu présenter leurs observations ou pour celles satisfaisant les demandes de la personne concernée.

La loi de transposition maintient la première interdiction. En revanche, conformément aux dispositions du règlement européen, elle assouplit les conditions de recours aux algorithmes, sans consentement des intéressés pour la prise de décisions emportant des effets juridiques.

Au titre des mesures appropriées pour la sauvegarde des droits et libertés et des intérêts légitimes de la personne concernée, auxquelles le règlement fait référence, il écarte d'abord tout traitement portant sur des données sensibles. Par ailleurs, il prévoit que l'administration doit informer l'usager, par une mention explicite, que la décision a été prise sur le fondement d'un algorithme. Il permet également à l'usager de se faire communiquer les règles de fonctionnement de ce traitement ainsi que les principales caractéristiques de sa mise en œuvre, sous la réserve des décisions reposant sur des règles dont la divulgation porterait atteinte

à des secrets protégés, tel que le secret de la défense nationale. Il impose, enfin, au responsable du traitement l'obligation de s'assurer de la maitrise du traitement de l'algorithme et de ses évolutions. En revanche, il écarte le droit pour la personne concernée d'obtenir une intervention humaine de la part du responsable du traitement.

Les requérants contestaient, dans son principe, le recours exclusif à un algorithme pour une prise de décision administrative et soutenaient, en outre, que l'administration renonçait, par ce biais, à son pouvoir d'appréciation du fait de l'existence d'algorithmes « auto-apprenants » susceptibles de réviser eux-mêmes les règles qu'ils appliquent.

Nous avons cependant validé les dispositions qui nous étaient déférées d'abord parce qu'elles sont conformes au règlement européen. Surtout nous avons constaté qu'elles prévoient bien des mesures appropriées pour la sauvegarde des droits et libertés et des intérêts légitimes de la personne concernée.

Néanmoins, nous avons tenu à reprendre dans notre décision les garanties énoncées, non sous la forme d'une réserve puisqu'elles figurent explicitement dans la loi, mais pour bien marquer que la conformité à la Constitution des dispositions en cause y est subordonnée. Nous avons également rappelé que les décisions prises sur le fondement d'un algorithme pouvaient faire l'objet d'un recours gracieux et juridictionnel, à l'occasion duquel une intervention humaine était nécessaire. Nous avons, en enfin, constaté que les dispositions de la loi qui imposent au responsable du traitement d'en conserver la maitrise et d'être en mesure d'en expliquer les règles de fonctionnement interdisaient l'usage d'algorithmes « auto-apprenants », qui modifient d'eux-mêmes les règles de traitement qu'ils appliquent.

Même si nous n'avons pas, en l'occurrence, prononcé de censure, cet aspect de notre décision est sans aucun doute le plus important pour marquer les limites qui s'imposent en matière de traitement de données personnelles.