10 mars 2022

Cour constitutionnelle

COMMUNIQUÉ DE PRESSE
ARRÊT 33/2022

La Cour rejette le recours contre la loi du 22 mai 2019 qui modifie la législation relative à la gestion des données à caractère personnel par les services de police

La loi du 22 mai 2019 concrétise le cadre général applicable au traitement des données à caractère personnel par les services de police. L'ASBL « Ligue des droits humains » demande l'annulation de plusieurs dispositions de cette loi.
La Cour rejette le recours. Elle juge que les règles applicables au traitement des données sensibles sont constitutionnelles. Elle rejette également les critiques dirigées contre l'interconnexion des banques de données policières. Enfin, la Cour considère que les règles relatives à l'accès direct des services de renseignement et de sécurité à la banque de données nationale générale (BNG) ménagent un juste équilibre entre le droit au respect de la vie privée et la protection de la sécurité nationale.

1. Contexte de l'affaire

En vue de l'exécution du RGPD (règlement (UE) 2016/679) et de la transposition de la directive « police » (directive (UE) 2016/680), le législateur a adopté la loi du 30 juillet 2018 « relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel ». Le titre 2 de cette loi fixe le cadre général applicable au traitement des données à caractère personnel par les services de police. Le législateur a encore concrétisé ce cadre en adoptant la loi du 22 mai 2019 « modifiant diverses dispositions en ce qui concerne la gestion de l'information policière ». L'ASBL « Ligue des droits humains » demande l'annulation de plusieurs dispositions de cette loi.

2. Examen par la Cour

Selon la partie requérante, plusieurs aspects de la loi du 22 mai 2019 portent atteinte au droit au respect de la vie privée, au droit à la protection des données à caractère personnel et au droit à un recours effectif. Elle développe plusieurs critiques concernant les données sensibles (2.1.), l'interconnexion des banques de données policières (2.2.) et l'accès direct des services de renseignement et de sécurité à la BNG (2.3.).

2.1. Les données sensibles

La partie requérante développe plusieurs critiques concernant les règles applicables aux données à caractère personnel qui sont, par nature, **particulièrement sensibles du point de vue des libertés et droits fondamentaux**, notamment les données de santé, les données génétiques et les données biométriques.

2.1.1. Les finalités du traitement des données de santé et des données génétiques (B.12-B.18)

La loi du 22 mai 2019 prévoit que le traitement des **données de santé** par les services de police peut uniquement intervenir « dans le but de comprendre le contexte lié à la personne concernée » et « pour assurer la sécurité et protéger la santé de toute personne susceptible d'entrer en contact avec les personnes concernées dans le cadre de l'intervention policière ». Selon la Cour, la première situation vise à garantir la sécurité et la santé de la personne concernée elle-même, tandis que la seconde situation garantit la sécurité et la santé des membres du personnel de la police et de toutes les autres personnes qui sont présentes lors de l'intervention. Sous réserve de cette interprétation, la Cour juge que les deux finalités sont suffisamment précises.

Le traitement des **données génétiques** par les services de police peut uniquement intervenir « dans le cadre de l'exercice des missions de police judiciaire et de l'application de la législation relative à la protection civile ». La Cour juge également que cette finalité est suffisamment précise.

2.1.2. Le délai de conservation des données biométriques et des données de santé (B.19-B.22)

La loi du 22 mai 2019 prévoit que les données sensibles sont traitées en complément ou en soutien du traitement principal portant sur d'autres catégories de données. Selon la Cour, le législateur n'a pas agi de manière déraisonnable en prévoyant pour ces données sensibles **les mêmes délais de conservation** que pour les données qu'elles complètent ou soutiennent.

2.1.3. Les garanties pour la personne concernée (B.23-B.26)

La Cour observe tout d'abord que le législateur n'autorise le traitement de données sensibles que s'il est **strictement nécessaire** à l'exercice des missions des services de police.

La Cour juge que **le législateur a prévu de manière suffisamment précise les exigences de qualité auxquelles les données sensibles doivent satisfaire** pour pouvoir être traitées par les services de police : (1) les données doivent être « adéquates », ce qui implique qu'elles doivent permettre de se former une idée correcte de la personne concernée et qu'il n'est dès lors pas permis de traiter uniquement les aspects défavorables à l'intéressé, (2) les données doivent être traitées « de manière licite et loyale » et doivent être « exactes et, si nécessaire, mises à jour », (3) la politique de protection des données doit indiquer les actions pour protéger le traitement des données et pour assurer la qualité des données traitées.

La Cour constate également que la consultation préalable de l'Organe de contrôle de l'information policière (l'Organe de contrôle) est requise avant tout traitement des données de santé « qui fera partie d'un nouveau fichier à créer » (article 59, § 1er, alinéa 1er, 2°, de la loi du 30 juillet 2018).

Enfin, la Cour juge que les **exigences de sécurisation** des données prévues par la législation sont suffisamment strictes.

2.2. L'interconnexion des banques de données policières (B.29-B.49)

La partie requérante dirige plusieurs critiques contre les habilitations aux ministres de l'Intérieur et de la Justice pour déterminer les règles d'accès des policiers aux banques de données policières et les modalités d'interconnexion de celles-ci.

La Cour rappelle en premier lieu que l'article 22 de la Constitution n'interdit pas au législateur d'accorder des délégations à un autre pouvoir, pour autant que ces délégations soient suffisamment définies et portent sur l'exécution de mesures dont les éléments essentiels ont été fixés à l'avance par le législateur. Dans cette affaire, la Cour juge que **les éléments essentiels ont été fixés par le législateur**. Le législateur prévoit en effet que les banques de données policières opérationnelles et les banques de données techniques sont uniquement accessibles aux policiers et que leurs profils et modalités d'accès sont entre autres déterminés sur la base du « besoin d'en connaître, en ce compris de la nécessité de croiser ou coordonner les données traitées », des finalités légales de chaque banque de données ainsi que de l'évaluation et de l'état de validation des données traitées. En outre, le législateur a établi le contenu minimal des directives portant sur les modalités d'interconnexion des banques de données. Enfin, le législateur a fixé les mesures de contrôle applicables.

Ensuite, la Cour juge que les notions de « règles d'accès », de « modalités relatives à l'interconnexion » et de « catégories de banques de données » sont **suffisamment précises**.

Enfin, la Cour juge que **la mesure est proportionnée**. Tout d'abord, le traitement des données à caractère personnel issues d'une interconnexion de banques de données est entouré des **garanties applicables à tout traitement** de données à caractère personnel par les services de police, notamment : (1) les données traitées doivent être adéquates, pertinentes et non excessives, (2) un délégué à la protection des données doit être désigné (3) les services de police sont contrôlés par l'Organe de contrôle, (4) la législation réglemente la période pendant laquelle des données à caractère personnel restent disponibles dans les banques de données policières, ainsi que l'archivage de ces données, la période d'archivage et l'accès à ces archives. De plus, le traitement par les services de police des données à caractère personnel issues d'une interconnexion de banques de données est entouré de **garanties particulières**. Celles-ci concernent les profils et les modalités d'accès aux banques de données interconnectées, ainsi que le contrôle par l'Organe de contrôle. En outre, les ministres de l'Intérieur et de la Justice doivent consulter l'Organe de contrôle avant d'autoriser toute interconnexion de banques de données et tout traitement impliquant une interconnexion.

2.3. L'accès direct des services de renseignement et de sécurité à la banque de données nationale générale (BNG) (B.56-B.69.5)

La partie requérante fait d'abord valoir que le droit d'accès direct à la BNG au profit des services de renseignement et de sécurité viole le principe de légalité formelle.

La Cour constate que le législateur a désigné les autorités qui peuvent accéder directement à la BNG, notamment les services de renseignement et de sécurité, et qu'il a prévu que cet accès direct ne peut leur être accordé que « dans le cadre de l'exercice de leurs missions légales ». En outre, le législateur a fixé les éléments essentiels des modalités de cet accès direct (article 44/11/12, § 2, de la loi du 5 août 1992 sur la fonction de police). Se référant à son arrêt n° 108/2016, la Cour juge que **le législateur pouvait habiliter le Roi à fixer les modalités relatives à cet accès direc**t. En outre, le Roi ne peut adopter ces modalités qu'après avoir reçu l'avis de l'Organe de contrôle.

La partie requérante fait ensuite valoir que l'accès direct à la BNG par les services de renseignement et de sécurité ne respecte pas le principe de finalité et qu'il constitue une ingérence disproportionnée dans le droit au respect de la vie privée.

La Cour constate que les dispositions attaquées autorisent les services de renseignement et de sécurité à accéder aux données contenues dans la BNG et qu'elles permettent ainsi que ces

données soient traitées pour les missions des services de renseignement. Celles-ci peuvent consister à rechercher, à analyser et à traiter le renseignement relatif à toute activité qui menace ou pourrait menacer la sûreté intérieure ou extérieure de l'État et à en informer les ministres compétents. Ces missions sont compatibles avec celles des services de police, en tant qu'elles participent à la sécurité nationale. En outre, les services de police et les services de renseignement et de sécurité sont contrôlés par le Comité permanent P, le Comité permanent R et l'Organe de contrôle. La Cour conclut que les dispositions attaquées ménagent **un juste équilibre entre le droit au respect de la vie privée et la protection de la sécurité nationale**.

3. Conclusion

La Cour rejette le recours, sous réserve de l'interprétation précitée relative aux finalités du traitement des données de santé et compte tenu de l'obligation pour les ministres de l'Intérieur et de la Justice de consulter l'Organe de contrôle avant d'autoriser toute interconnexion de banques de données et tout traitement impliquant une interconnexion.

La Cour constitutionnelle est la juridiction qui veille au respect de la Constitution par les différents législateurs en Belgique. La Cour peut annuler, déclarer inconstitutionnels ou suspendre des lois, des décrets ou des ordonnances en raison de la violation d'un droit fondamental ou d'une règle répartitrice de compétence.

Ce communiqué de presse, rédigé par la cellule « médias » de la Cour, ne lie pas la Cour constitutionnelle. Le texte de l'arrêt est disponible sur le site web de la Cour constitutionnelle.

Contact presse : Martin Vrancken | 02/500.12.87 | Romain Vanderbeck | 02/500.13.28

Suivez la Cour via Twitter @ConstCourtBE