



Cour constitutionnelle

COMMUNIQUÉ DE PRESSE ARRÊT 2/2021

La loi qui impose d'intégrer des empreintes digitales sur la carte d'identité ne viole pas le droit au respect de la vie privée et à la protection des données à caractère personnel

La Cour rejette les recours en annulation de l'article 27 de la loi du 25 novembre 2018, qui prévoit l'intégration de l'image numérisée de deux empreintes digitales sur la carte d'identité. Selon la Cour, l'ingérence qu'entraîne la mesure dans le droit au respect de la vie privée et à la protection des données à caractère personnel est raisonnablement justifiée par l'objectif de lutter contre la fraude à l'identité. Elle n'emporte par ailleurs pas d'effets disproportionnés sur les droits des personnes concernées, compte tenu des garanties prévues. En effet, la disposition attaquée n'instaure pas un registre central des empreintes digitales de l'ensemble des détenteurs d'une carte d'identité. Les autorités habilitées à lire ces données sont limitativement énumérées. Pour le reste, il appartient au pouvoir exécutif de prendre les mesures techniques nécessaires en vue d'assurer la sécurisation des données. La Cour juge qu'il n'est pas nécessaire d'interroger à titre préjudiciel la Cour de justice de l'Union européenne sur la validité du règlement (UE) 2019/1157, qui prévoit une mesure analogue au niveau européen, ni sur l'interprétation du droit de l'Union.

1. Contexte des affaires

La Cour est saisie de cinq recours en annulation de l'article 27 de la loi du 25 novembre 2018 portant des dispositions diverses concernant le Registre national et les registres de population. Ces recours sont introduits par le Parti Libertarien, les ASBL « Liga voor Mensenrechten » et « Ligue des droits humains », ainsi que plusieurs particuliers. Les requérants considèrent que la disposition attaquée, qui prévoit l'intégration, sur la carte d'identité, de l'image numérisée de deux empreintes digitales, viole le droit au respect de la vie privée et à la protection des données à caractère personnel.

Quelques mois plus tard a été adopté le règlement (UE) 2019/1157 du 20 juin 2019 « relatif au renforcement de la sécurité des cartes d'identité des citoyens de l'Union (...) », qui prévoit une mesure similaire au niveau européen. Le règlement est entré en vigueur le 1er août 2019 et sera applicable à partir du 2 août 2021.

2. Examen par la Cour

2.1. Quant à la recevabilité

La disposition attaquée s'applique à tous les Belges de 12 ans et plus. Elle affecte donc directement et défavorablement la situation des requérants particuliers, de sorte que leurs

recours sont recevables. L'entrée en vigueur, entretemps, du règlement (UE) 2019/1157 n'y change rien.

À l'occasion de l'examen de la recevabilité de plusieurs moyens invoqués par les requérants, la Cour juge que **le règlement général sur la protection des données (RGPD) n'impose pas au législateur de réaliser une analyse d'impact** sur la protection des données **lorsqu'il élabore une loi qui prévoit un traitement de données susceptible d'engendrer un risque élevé** pour les droits des personnes concernées, pour autant qu'une telle analyse d'impact ait lieu avant le traitement proprement dit. Le grief pris de l'absence d'une telle analyse d'impact par le législateur doit donc être rejeté.

2.2. Quant au fond

2.2.1. Le prélèvement des empreintes digitales et la conservation de l'image numérisée de celles-ci sur la carte d'identité, en ce compris les aspects techniques (B.18-B.36)

Les parties requérantes font valoir que l'ingérence qu'entraîne la disposition attaquée dans les droits des personnes concernées n'est pas décrite suffisamment précisément. Elle ne serait en outre pas nécessaire et entraînerait des effets disproportionnés.

Selon la Cour, la disposition attaquée entraîne une **ingérence dans le droit au respect de la vie privée et à la protection des données à caractère personnel** (article 22 de la Constitution, article 8 de la Convention européenne des droits de l'homme et articles 7 et 8 de la Charte des droits fondamentaux de l'UE). Elle **poursuit** cependant **des objectifs légitimes**, à savoir renforcer la **lutte contre la fraude à l'identité** et **prévenir les infractions liées à cette fraude**. Par ailleurs, elle met en œuvre, de manière anticipée, le règlement (UE) 2019/1157, qui vise aussi à « renforcer la sécurité pour faciliter l'exercice des droits à la libre circulation par les citoyens de l'Union et les membres de leur famille ». La Cour renvoie à l'arrêt de la Cour de justice de l'Union européenne du 17 octobre 2013, [Schwarz c. Stadt Bochum](#), par lequel cette Cour a validé le règlement européen prévoyant une mesure analogue pour les passeports.

La Cour estime que la disposition attaquée est **apte** à réaliser ces objectifs, puisque l'ajout des empreintes digitales réduit le risque de falsification et d'utilisation frauduleuse des cartes d'identité et facilite la tâche des autorités qui examinent l'authenticité de celles-ci aux frontières.

La Cour relève que **la disposition attaquée détermine les aspects suivants** : 1) les données visées, à savoir l'image numérisée de deux empreintes digitales, 2) la durée maximale de conservation de ces données en vue de la fabrication et de la délivrance de la carte d'identité (3 mois), après quoi les données doivent être détruites définitivement, et 3) les instances habilitées à lire les empreintes. La disposition attaquée prévoit aussi que les données sont ensuite stockées **uniquement sur la carte d'identité** et qu'elles sont lisibles exclusivement de manière électronique. Ensuite, **la délégation au Roi porte sur des aspects limités**. La mesure est donc **suffisamment prévisible** pour les personnes concernées.

La Cour observe que les cartes d'identité sont fréquemment utilisées pour voyager dans l'Union, voire en dehors, ou pour obtenir un passeport. **Une certaine analogie entre les passeports et les cartes d'identité est permise**, mais **le test de nécessité et de proportionnalité doit être plus strict pour les cartes d'identité**, vu leur importance dans la vie quotidienne et leur caractère obligatoire. Lors du contrôle de la nécessité et de la proportionnalité de la mesure, la Cour tient compte de l'arrêt [Schwarz c. Stadt Bochum](#) précité.

La Cour constate que la disposition attaquée **n'affecte pas le contenu essentiel des droits** concernés. Elle remarque à cet égard que **la disposition attaquée n'établit pas un registre central des empreintes digitales de l'ensemble des détenteurs d'une carte d'identité**, mais qu'elle prévoit uniquement l'intégration de l'image numérisée des empreintes digitales sur la carte d'identité. Selon la Cour, il appartient au juge compétent de vérifier si le Roi, dans l'exécution des délégations qui lui ont été conférées, a pris les mesures techniques et organisationnelles adéquates en vue de la sécurisation des données. Sous cette réserve, **le risque d'abus dénoncé par les parties requérantes n'est pas suffisamment caractérisé.**

2.2.2. La conservation centralisée des empreintes digitales en vue de la fabrication et la délivrance de la carte d'identité (B.37-B.39)

Les parties requérantes critiquent la conservation centralisée des empreintes digitales en vue de la fabrication et de la délivrance de la carte d'identité, au motif qu'elle ne serait pas nécessaire et que l'intégrité et la confidentialité des données ne seraient pas assurées.

La Cour juge que **la centralisation des empreintes digitales en vue de la fabrication et de la délivrance** de la carte d'identité, plutôt qu'une conservation au sein de chaque commune, **est justifiée par la nécessité de garantir la sécurité et l'intégrité des données.** À cet égard, la durée maximale de conservation des données, de 3 mois, n'est pas manifestement excessive. Pour le reste, le Roi doit prendre les mesures adéquates en vue de la sécurisation des données.

2.2.3. La lecture des empreintes digitales (B.40-B.44)

En ce qui concerne les critiques des parties requérantes concernant la lecture des empreintes digitales, la Cour juge que les modalités concrètes de cette lecture relèvent de l'exécution de la loi, qui est de la compétence du Roi. Par ailleurs, **les instances habilitées à lire les empreintes digitales ne peuvent pas les enregistrer.**

Selon la Cour, **la finalité de la lecture découle logiquement de l'objet de la mesure ainsi que des missions que les instances habilitées assument.** Ainsi, la disposition attaquée doit être raisonnablement interprétée comme n'autorisant la lecture par le personnel chargé du contrôle aux frontières que dans le cadre du contrôle aux frontières. L'habilitation aux services de police est aussi suffisamment délimitée. En outre, **lors de la phase de fabrication et de délivrance de la carte d'identité, la lecture des données n'est permise qu'aux seules fins de cette fabrication et de cette délivrance**, ce qui exclut toute consultation par la police de ces données.

Quant au risque d'abus invoqué par les parties requérantes, la Cour juge que **les instances habilitées à lire les empreintes digitales le sont uniquement dans le cadre de l'exercice de leurs fonctions légalement décrites.** Elles doivent respecter, ce faisant, les règles de protection des données à caractère personnel, sous le contrôle du juge compétent.

Enfin, la disposition attaquée ne permet pas le croisement des données afin d'identifier un individu, dès lors que les empreintes digitales ne peuvent pas être enregistrées lors de la lecture. Par ailleurs, les empreintes digitales ne peuvent pas être lues à l'insu de l'intéressé puisque leur consultation suppose un contact direct avec le citoyen dont l'identité est vérifiée.

3. Conclusion

La Cour **rejette** les recours. Dès lors que l'examen des griefs n'a pas soulevé de doute sur la validité d'une des mesures de la disposition attaquée trouvant son équivalent dans le règlement

(UE) 2019/1157 ou sur l'interprétation du droit de l'Union, la Cour refuse de poser une question préjudicielle à la CJUE.

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](#)