L’enregistrement des empreintes digitales sur la carte d’identité est-il contraire au droit à la vie privée des citoyens ?

Degrave, Elise; Mont, Julie

Published in:
Revue du Droit des Technologies de l'information

Publication date:
2021

Document Version
le PDF de l'éditeur

Note d'observations[1]

L'enregistrement des empreintes digitales sur la carte d'identité est-il contraire au droit à la vie privée des citoyens ?

I. LE MÉCANISME : LES EMPREINTES DIGITALES INTEGRÉES À LA CARTE D'IDENTITÉ ÉLECTRONIQUE

1. La carte d'identité. L'obligation de délivrer aux citoyens belges une carte d'identité est prévue par la loi du 19 juillet 1991[2]. En 2003, la carte d'identité s'est modernisée et les citoyens détiennent depuis lors une carte d'identité électronique (ci-après « l'e-*id.* »)[3]. À l'occasion d'une loi adoptée le 25 novembre 2018, le législateur a introduit une nouvelle donnée sur l'e-*id.*, à savoir l'image numérisée des empreintes digitales de l'index de la main gauche et de la main droite[4].

La finalité poursuivie par l'enregistrement de cette information n'apparaît pas dans la loi. Pour comprendre l'objectif poursuivi par le législateur, il y a lieu de lire les travaux préparatoires de la loi du 25 novembre 2018, qui font état, notamment, de la volonté de lutter contre la fraude à l'identité[5], en permettant aux services de police de vérifier l'exactitude du lien entre la carte d'identité et le porteur de celle-ci[6]. Nous y reviendrons *infra*.

L'arrêté royal du 25 mars 2003 relatif aux cartes d'identité précise qu'il appartient au ministre de l'Intérieur de fixer la date à laquelle les cartes d'identité doivent comporter ces empreintes[7]. Le 15 janvier 2021, la ministre de l'Intérieur Annelies Verlinden a adopté un arrêté ministériel qui fixe rétroactivement à la date du 10 décembre 2020 la date à partir de laquelle « toute carte d'identité demandée par un Belge résidant en Belgique doit comporter les empreintes digitales »[8]. Le citoyen belge qui doit se créer ou renouveler sa carte d'identité est donc désormais tenu de fournir ses empreintes digitales.

2. La numérisation des empreintes. Concrètement, lorsque le citoyen se présente à l'administration communale, le préposé numérise ses empreintes digitales au moyen de capteurs. L'image numérisée des empreintes est transmise par les services du Registre national au producteur de la carte d'identité afin d'être intégrées électroniquement à celle-ci[9]. La loi prévoit que l'image numérisée des empreintes ne peut être conservée que durant maximum trois mois, c'est-à-dire la période nécessaire

1 Elise Degrave et Julie Mont, respectivement professeure à la Faculté de droit de l'UNamur, directrice de recherches au Nadi/Crids et co-directrice de la Chaire Egouvernement de l'UNamur ; assistante à la Faculté de droit de l'UNamur, chercheuse au Nadi/Crids et avocate au barreau de Namur.

2 Loi du 19 juillet 1991 relative aux registres de la population, aux cartes d'identité, aux cartes des étrangers et aux documents de séjour, *M.B.*, 3 septembre 1991.

3 À ce sujet voy. E. Degrave et J. Mont, « La carte d'identité électronique à la lumière du droit à la protection de la vie privée », *Revue de droit communal*, 2021, pp. 3-15.

4 Loi du 25 novembre 2018 portant des dispositions diverses concernant le Registre national et les registres de population, *M.B.*, 13 décembre 2018, article 27.

5 Projet de loi du 23 juillet 2018 portant des dispositions diverses concernant le Registre national et les registres de population, Exposé des motifs, *op. cit.*, p. 34.

6 *Ibid.*, p. 34.

7 Arrêté royal relatif aux cartes d'identité du 25 mars 2003, *M.B.*, 28 mars 2003, article 3, § 5.

8 Arrêté ministériel fixant la date d'entrée en vigueur de l'article 3, § 5, al. 1, de l'arrêté royal du 25 mars 2003 relatif aux cartes d'identité, *M.B.*, 19 février 2021, p. 16054.

9 Arrêté royal relatif aux cartes d'identité du 25 mars 2003, *op. cit.*, article 3, § 5.

pour fabriquer et délivrer la carte au citoyen, dans une « banque de données centralisée », dont la loi ne dit mot.

Il est à noter qu'il s'agit ici d'enregistrer les empreintes digitales de l'ensemble des citoyens et de placer leur image numérisée sur la puce de l'e-*id*. Il s'agit donc d'un procédé différent de celui utilisé par les services de police qui, dans le cadre de leurs missions de police administrative et judiciaire, ont la possibilité de collecter et traiter, pourvu qu'elles soient pertinentes, adéquates et proportionnées, les empreintes digitales des personnes impliquées dans des infractions de police administrative ou judiciaire[10]. Ces données sont stockées dans des banques de données opérationnelles, dont la banque de données Nationale Générale (« B.N.G. ») qui comprend les données pouvant être partagées par l'ensemble des services de police. Ces données sont conservées pendant plusieurs années et, pour celles stockées dans la B.N.G., archivées ensuite pendant une durée pouvant aller jusqu'à 30 ans[11].

3. Contrôle des fraudes. Une fois la carte fabriquée, les empreintes sont stockées sur la puce de celle-ci et ne peuvent être lues que par certaines instances listées par la loi, à savoir le personnel communal, les services de police, le personnel chargé du contrôle aux frontières en Belgique et à l'étranger, le personnel de l'Office des étrangers, les membres du SPF Affaires étrangères et le personnel diplomatique et consulaire, ainsi que l'entreprise chargée de la production des cartes d'identité[12].

L'objectif avancé par le législateur est donc, en cas de contrôle, de pouvoir éviter la fraude à l'identité via la ressemblance (fraude dite « *look alike* »), qui consiste à exploiter une ressemblance physique pour usurper l'identité d'une personne à qui l'on ressemble lors d'un contrôle ou pour obtenir de nouveaux documents d'identité. Si, lors d'un contrôle par une instance compétente, il devait être constaté que les empreintes digitales présentes sur la carte ne correspondent pas aux empreintes digitales de la personne en face de soi, l'identité de cette personne fera l'objet d'un contrôle approfondi sur la base d'autres données d'identification.

Nous verrons toutefois dans les lignes qui suivent qu'aussi louable soit cet objectif, notamment pour la sécurité de l'État, il n'en demeure pas moins que la collecte et le traitement des empreintes digitales des citoyens consistent en une ingérence dans leur droit à la vie privée, qui nécessite des balises claires et solides.

4. Recours. C'est dans ce contexte qu'en février, mars et juin 2019, cinq recours en annulation ont été introduits à la Cour constitutionnelle, contre l'article 27 – disposition qui vise à introduire l'image numérisée des empreintes des citoyens sur l'e-*id*. – de la loi du 25 novembre 2018[13]. Les requérants ont en

10 Loi du 5 août 1992 sur la fonction de police, *M.B.*, 22 décembre 1992, article 44/1.

11 *Ibid.*, article 44/11/3*bis*.

12 Loi du 25 novembre 2018 portant des dispositions diverses concernant le Registre national et les registres de population, *op. cit.*, article 27, 2°.

13 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, introduit par le parti libertarien et Baudoin Collard, n° rôle 7125 ; 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, introduit par Matthias Dobbelaere-Welvaert et autres, n° rôle 7150 ; 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, introduit par l'ASBL « Liga voor Mensenrechten », n° rôle 7202 ; 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, introduit par l'ASBL « Ligue des droits humains », n° rôle 7203 ; Recours en annulation de l'article 27 de la loi du 25 novembre 2018 portant des

effet estimé que cet article, imposant désormais aux citoyens de fournir leurs empreintes digitales, portait atteinte à leur droit à la vie privée. Leurs recours ont été joints, et ont donné lieu à l'arrêt de la Cour du 14 janvier 2021, que nous analyserons ci-après[14].

II. LA QUESTION : LES EMPREINTES DIGITALES SUR L'E-*ID.*, UNE INGÉRENCE DANS LA VIE PRIVÉE DES CITOYENS ?

5. Données à caractère personnel. Les empreintes digitales sont des données à caractère personnel puisqu'elles contiennent des informations sur les citoyens et permettent de les identifier de manière précise. Les empreintes digitales sont des « données biométriques » au sens du RGPD[15], qui leur accorde une protection spécifique puisqu'il interdit, par principe, le traitement de telles données et ne l'autorise que dans des conditions strictes, notamment si le traitement répond à un motif d'intérêt public important[16].

En conséquence, le traitement de telles données doit être strictement encadré, aux fins de respecter le droit à la protection des données à caractère personnel des citoyens.

6. Ingérence. La Cour confirme qu'en ce qu'elle prévoit le prélèvement de deux empreintes digitales et l'image numérisée de celles-ci sur la carte d'identité, la disposition attaquée entraîne une ingérence dans le droit au respect de la vie privée et dans le droit à la protection des données, tels qu'ils sont garantis, notamment, par l'article 22 de la Constitution et l'article 8 de la Convention européenne des droits de l'homme[17].

La Cour rappelle, conformément à sa jurisprudence constante, qu'une ingérence dans la vie privée n'est admissible et autorisée que si la mesure mise en place poursuit un objectif légitime, qui doit, selon les termes de la Convention européenne des droits de l'homme, être un besoin social impérieux dans une société démocratique. Cet objectif doit également constituer un motif d'intérêt public au sens de l'article 9 du RGPD, puisque les empreintes digitales sont des données biométriques[18].

L'ingérence dans le droit à la vie privée doit en outre être proportionnée à l'objectif légitime poursuivi, c'est-à-dire que les mesures liées au traitement de données doivent être pertinentes, au sens où elles doivent être susceptibles d'atteindre l'objectif poursuivi, mais elles doivent également être nécessaires. Pour s'en assurer, il faut vérifier qu'il n'existe pas de mesure alternative, qui créerait moins de dommages collatéraux, tout en atteignant le but poursuivi[19].

Enfin, et en vertu du principe de légalité, l'ingérence doit être organisée par le législateur, de manière claire et précise[20].

Il appartient donc à la Cour de vérifier si cette ingérence est, dans le cas d'espèce, admissible.

dispositions diverses concernant le Registre national et les registres de population, introduit par Siham Najmi et John Pitseys, en leur qualité de représentants légaux de leur fils Samuel Pitseys Najmi, n° rôle 7211.

14 Cour const., arrêt n° 2/2021 du 14 janvier 2021 (n°s de rôle 7125, 7150, 7202, 7203 et 7211), disponible à l'adresse : https://www.const-court.be/public/f/2021/2021-002f.pdf.

15 RGPD, article 4, 14) : les données biométriques sont « les données à caractère personnel résultant d'un traitement technique spécifique, relatives aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique, qui permettent ou confirment son identification unique, telles que des images faciales ou des données dactyloscopiques ».

16 RGPD, article 9, 1).

17 Cour const., arrêt n° 2/2021 du 14 janvier 2021 précité, B.19.1.

18 *Ibid.*, B.19.2.

19 *Ibid.*, B.25.2.

20 *Ibid.*, B.22.1.

III. L'OBJECTIF POURSUIVI PAR L'ENREGISTREMENT DES EMPREINTES SUR L'E-*ID.*

7. Objectif légitime. La Cour vérifie premièrement si l'ingérence poursuit un objectif légitime.

La Cour se penche sur les travaux préparatoires de la loi du 25 mai 2018 reprenant l'objectif poursuivi par la disposition attaquée, qui est de permettre une identification plus précise des individus pour renforcer la lutte contre la fraude à l'identité (fraude basée sur la ressemblance ou « fraude *look alike* » et obtention frauduleuse de documents authentiques)[21]. Seuls des cas limités de fraude sont donc visés.

Selon la Cour, en poursuivant cet objectif, la Belgique anticipe la mise en œuvre du règlement européen du 20 juin 2019 « relatif au renforcement de la sécurité des cartes d'identité des citoyens de l'Union (…) »[22], qui sera applicable dans l'Union européenne à partir du 2 août 2021[23]. Il impose que les cartes d'identité nationales contiennent la photo de leur titulaire mais également « deux empreintes digitales dans des formats numériques interopérables »[24]. L'objectif annoncé est de « renforcer la sécurité des cartes d'identité et des cartes de séjour »[25] en combinant « de manière appropriée une identification et une authentification fiables avec une réduction du risque de fraude »[26]. Le législateur européen s'est basé sur le constat que les documents de voyage délivrés dans l'Union européenne sont très prisés des fraudeurs et que la fraude basée sur la ressemblance et l'obtention frauduleuse de documents authentiques ont augmenté ces dernières années[27]. La validité de ce règlement était également, dans le cadre des recours devant la Cour, contestée par les requérants, qui l'estimaient contraire au droit au respect de la vie privée et à la protection des données ainsi qu'au principe d'égalité, en ce qu'il crée une discrimination entre les citoyens de l'Union selon qu'ils sont soumis, ou non, à l'obligation de disposer d'une carte d'identité[28]. Les requérants sollicitaient de la Cour qu'elle pose plusieurs questions liées à la validité de ce règlement à la Cour de justice[29].

La Cour considère que l'objectif poursuivi par la mesure – basé donc sur l'objectif poursuivi par le règlement UE – est légitime et constitue un objectif d'intérêt général reconnu par l'Union[30]. La Cour applique la jurisprudence de la Cour de justice de l'Union européenne, qui a considéré que le règlement européen n° 2252/2004 qui prévoit l'intégration des empreintes digitales sur les passeports pour prévenir la falsification et l'utilisation frauduleuse de ceux-ci, poursuit un objectif d'intérêt général reconnu par l'Union. Elle rejette également les demandes des requérants et refuse de poser quelque question préjudicielle à la Cour de justice, estimant que l'examen des griefs n'a pas soulevé de doute concernant la validité de la disposition attaquée, ni concernant le règlement 2019/1157[31].

21 *Ibid.*, B.20.1.

22 Règlement (UE) 2019/1157 du Parlement européen et du Conseil du 20 juin 2019 relatif au renforcement de la sécurité des cartes d'identité des citoyens de l'Union et des documents de séjour délivrés aux citoyens de l'Union et aux membres de leur famille exerçant leur droit à la libre circulation, *J.O.*, 12 juillet 2019, L 188/67 (ci-après « Règlement 2019/1157 »).

23 Cour const., arrêt n° 2/2021 du 14 janvier 2021 précité, B.20.1.

24 Règlement 2019/1157, article 3.5.

25 Règlement 2019/1157, considérant 18.

26 *Idem.*

27 Communication de la Commission au Parlement européen et au Conseil de 2016 (COM 2016/790), citée par la Cour, au B.20.1 de l'arrêt.

28 Cour const., arrêt n° 2/2021 du 14 janvier 2021 précité, A.33.1.

29 À ce sujet voy. E. Degrave et J. Mont, « La carte d'identité électronique à la lumière du droit à la protection de la vie privée », *op. cit.*, pp. 7-8.

30 Cour const., arrêt n° 2/2021 du 14 janvier 2021 précité, B.20.2.

31 *Ibid.*, B.45.2.

8. Intérêt public important. La Cour ajoute que l'objectif poursuivi est d'intérêt public important au sens de l'article 9 du RGPD, ce qui, selon elle et sans autre précision, « se déduit » de l'adoption du règlement européen 2019/1157[32].

9. La lutte contre la fraude en pratique. Outre la légitimité de l'objectif poursuivi par la disposition, il y a lieu de s'interroger sur la manière dont on va veiller à atteindre, en pratique, cet objectif de lutter contre la fraude à l'identité en contrôlant les cartes d'identité.

10. Enregistrement des empreintes. À ce sujet, les requérants faisaient grief à la disposition attaquée de ne pas déterminer la technique ou la méthode par laquelle les empreintes allaient être enregistrées et lues et de ne pas interdire l'enregistrement des données à cette occasion.

La Cour rappelle qu'il appartient au Roi de prendre les mesures techniques adéquates à cet effet, et précise que les travaux préparatoires de la loi du 25 mai 2018 prévoient que les empreintes seront protégées par un certificat permettant une lecture uniquement par des lecteurs autorisés[33]. Par ailleurs, la disposition attaquée habilite certaines instances à lire les empreintes, mais pas à les enregistrer, de sorte que la Cour en déduit que l'enregistrement de ces données lors de la lecture n'est pas permise[34]. Il s'agit d'une interprétation de la Cour.

11. Lecture des empreintes. Deuxièmement, les requérants reprochaient à la disposition de ne pas préciser en quoi consiste la lecture des empreintes digitales, ce qui confère une très large habilitation aux autorités concernées s'agissant de l'accès aux données et à leur utilisation ultérieure. Rien n'est prévu dans la loi concernant le but de la lecture par les agents chargés du contrôle aux frontières (y compris les agents étrangers qui pourraient ressortir d'une firme privée) et le traitement des empreintes par la police[35]. La Cour se contente d'indiquer que la finalité de lecture des empreintes découle de l'objet de la mesure et des missions assurées par les instances habilitées à y procéder. S'agissant des contrôles, il semble clair pour la Cour que la disposition autorise la lecture uniquement dans le cadre des contrôles aux frontières et à cette seule fin, ainsi que par les services de police à des fins délimitées et découlant de motifs d'intérêt public important[36]. Enfin, la Cour rappelle que l'habilitation ne vaut que pour la lecture des empreintes et non l'enregistrement de données, ce qui exclut toute utilisation ultérieure[37]. À nouveau, il s'agit d'une interprétation de la Cour.

12. L'accès durant la fabrication. Les requérants soulevaient également le fait que la disposition attaquée permet aux instances énumérées par la loi de lire les empreintes une fois l'e-*id.* délivrée au citoyen, mais aussi lors de la phase de fabrication, en accédant à la banque de données centralisée qui conserve temporairement les informations[38].

À ce propos, la Cour rejoint la position du Conseil des ministres qui assure que durant la phase de fabrication, les données peuvent être lues uniquement pour cette fin et que dès lors, les services de police et les contrôleurs aux frontières ne peuvent consulter les empreintes digitales (stockées dans la base de données) lors de ce processus[39].

13. Croisement de données. Enfin, les requérants relevaient au titre de dernier argument le

32 *Ibid.*, B.20.2.
33 *Ibid.*, B.41.2.
34 *Ibid.*, B.41.3.
35 *Ibid.*, B.42.1.
36 *Ibid.*, B.42.2.1 à B.42.2.4.
37 *Ibid.*, B.42.2.5.
38 *Ibid.*, B.43.1.
39 *Ibid.*, B.43.2.

fait que la disposition permettait une lecture des empreintes « à grande échelle, sans contact et secrètement », notamment par la police, et permettait également un croisement de données avec d'autres informations pour identifier un individu[40].

La Cour estime qu'un tel croisement de données n'est pas possible, puisque les empreintes ne peuvent être enregistrées lorsqu'elles sont lues, et que cette lecture ne se fait jamais à l'insu de l'intéressé qui aura toujours un contact avec l'autorité qui le contrôle et à qui il doit présenter sa carte[41].

Pour la lecture des empreintes à grande échelle, la Cour rappelle que les instances habilitées à lire les empreintes le sont dans le cadre de missions bien déterminées et doivent, dans le cadre de cette habilitation, respecter les principes issus du RGPD notamment s'agissant du traitement de données sensibles. Pour la Cour, il s'agit d'une question de respect de la loi par ces autorités, pour laquelle elle n'est pas compétente[42].

IV. LA PROPORTIONNALITÉ DE LA MESURE

14. Un examen délicat. Après avoir examiné l'objectif poursuivi, la Cour entame l'examen de proportionnalité de la mesure. Il s'agit de s'assurer que l'insertion des empreintes digitales sur l'e-*id.* est une mesure pertinente – c'est-à-dire susceptible d'atteindre l'objectif poursuivi –, nécessaire – ce qui suppose qu'il n'existe pas de mesure alternative qui crée moins de dégâts collatéraux – et que la mesure respecte la proportionnalité au sens strict en incarnant un équilibre raisonnable entre l'objectif poursuivi et l'impact de la mesure sur les libertés.

Évaluer la proportionnalité d'une mesure est une tâche délicate « car marquée, inévitablement, par l'imprévisibilité et donc l'insécurité »[43] propre au contrôle de la proportionnalité de la mesure. Il en va d'autant plus ainsi lorsqu'il s'agit d'évaluer une technologie, puisque cela suppose notamment que l'on soit éclairé sur son efficacité et donc, sur son fonctionnement.

D'emblée, il est piquant de constater que tant le législateur belge que la Cour constitutionnelle affirment que l'insertion des empreintes digitales sur l'e-*id.* est une mesure pertinente, nécessaire et proportionnée. Pourtant, à la lecture des travaux préparatoires de la loi, et de l'arrêt commenté, on peut légitimement se demander quelles sont les preuves et analyses concrètes ayant nourri les affirmations du législateur et de la Cour constitutionnelle sur cette technologie peu familière des juristes.

Un outil aurait pourtant pu les aider considérablement à donner une assise convaincante à leur analyse. Cet outil s'appelle l'analyse d'impact auquel on consacre les lignes qui suivent.

A. L'analyse d'impact

15. Article 35 RGPD. L'analyse d'impact est imposée par le Règlement général pour la protection des données, notamment lorsqu'un État traite, à grande échelle, des données biométriques, comme c'est le cas en l'espèce[44]. Cette analyse d'impact doit amener l'auteur d'une mesure à faire le point sur la technologie qu'il souhaite mettre en place, en en évaluant

40 *Ibid.*, B.44.1
41 *Ibid.*, B.44.3
42 *Ibid.*, B.44.2.

43 B. Renauld et S. Van Drooghenbroeck, « Le principe d'égalité et de non-discrimination », in M. Verdussen et N. Bonbled (dir.), *Les droits constitutionnels en Belgique*, Bruxelles, Bruylant, 2011, vol. 2, p. 593.

44 Art. 35.3.b) du RGPD qui dispose :
« l'analyse d'impact relative à la protection des données visée au paragraphe 1 est, en particulier, requise dans les cas suivants :
b) le traitement à grande échelle de catégories particulières de données visées à l'article 9, paragraphe 1 (…) ».

les avantages et les risques. L'analyse de la nécessité et de la proportionnalité de la technologie mise en place doit d'ailleurs être effectuée à cette occasion, comme le mentionne explicitement le RGPD, de manière à amener le responsable du traitement à choisir la technologie la plus adéquate par rapport à l'objectif poursuivi[45].

Rappelons que le RGPD est directement applicable en Belgique. Au-delà de l'obligation du législateur de s'y conformer, l'analyse d'impact est une démarche très intéressante pour amener à réfléchir aux impacts d'une technologie, choisir la solution la plus adéquate, et, partant, inspirer la confiance des citoyens directement concernés par les mesures envisagées, en démontrant, par l'analyse d'impact, que les mesures ont été minutieusement analysées et que les mesures les moins liberticides ont été privilégiées.

En l'occurrence, le législateur n'a pas effectué cette analyse d'impact avant de décider de l'insertion obligatoire des empreintes digitales sur l'e-*id.* de toute de la population, ce que les requérants n'ont pas manqué de critiquer.

La Cour répond à cet argument de manière étonnante. Elle affirme qu'une analyse d'impact « lors de l'élaboration d'une disposition législative » relative à un traitement présentant des risques élevés pour les droits et libertés des citoyens « est facultative » au motif que, selon l'article 35, paragraphe 10, du RGPD, une analyse d'impact ne doit pas être effectuée lorsque le traitement envisagé « a une base juridique dans le droit de l'Union ou dans le droit de l'État membre ».

La Cour ne précise toutefois pas quelle est la « base juridique dans le droit de l'Union » et/ou dans le droit belge, sur laquelle le législateur peut se fonder en l'espèce. S'agirait-il alors de la disposition en cours d'élaboration, ce qui reviendrait à assimiler « disposition en cours d'élaboration » et « base juridique existante » ? Ce serait là assez incohérent. En effet, au moment de l'élaboration de la disposition législative visant à insérer les empreintes digitales sur l'e-*id.*, il n'y avait pas encore de base juridique existante organisant cette insertion puisque celle-ci était précisément en cours d'élaboration.

16. Lacune législative et interprétation. À notre sens, l'article 35 RGPD souffre d'une lacune législative en ce qu'il ne répond pas explicitement à la question de savoir si une analyse d'impact doit être effectuée pour les traitements mis en place par l'État via une disposition législative en cours d'élaboration, dans l'hypothèse où il n'y pas de base juridique existante ou que celle-ci est imprécise[46]. C'est probablement ce qui a motivé les requérants

[45] Plus précisément, selon l'article 35.7 RGPD, l'analyse d'impact doit contenir au moins les éléments suivants :
a) une description systématique des opérations de traitement envisagées et des finalités du traitement, y compris, le cas échéant, l'intérêt légitime poursuivi par le responsable du traitement ;
b) une évaluation de la nécessité et de la proportionnalité des opérations de traitement au regard des finalités ;
c) une évaluation des risques pour les droits et libertés des personnes concernées conformément au paragraphe 1 ; et
d) les mesures envisagées pour faire face aux risques, y compris les garanties, mesures et mécanismes de sécurité visant à assurer la protection des données à caractère personnel et à apporter la preuve du respect du présent règlement, compte tenu des droits et des intérêts légitimes des personnes concernées et des autres personnes affectées.

[46] Rappelons qu'en droit belge, il découle de l'article 22 de la Constitution que chaque ingérence dans la vie privée des citoyens doit être organisée par une loi claire et prévisible, ce qui signifie qu'elle doit mentionner tous les éléments essentiels des traitements de données mis en place (pour plus d'informations, comme l'affirme notamment la Cour constitutionnelle dans sa jurisprudence constante à ce sujet, voy. E. Degrave, *L'e-gouvernement et la protection de la*

à demander qu'une question préjudicielle soit posée par la Cour constitutionnelle à la Cour de justice de l'Union européenne. La Cour constitutionnelle a malheureusement refusé de le faire, estimant que l'article 35 du RGPD « ne laisse place à aucun doute raisonnable »[47].

Pourtant, des doutes raisonnables ne sont pas à exclure d'emblée. Ainsi qu'on vient de le dire, l'article 35 RGPD ne dit rien de l'obligation, ou non, d'effectuer une analyse d'impact au stade de l'élaboration d'une disposition législative. Toutefois, un raisonnement par la *ratio legis* – la raison d'être – de l'article 35 RGPD, peut éclairer la réflexion. Si l'analyse d'impact doit être effectuée, c'est pour aider le responsable du traitement – en l'occurrence, l'État – à choisir la solution la plus juste et à démontrer, au public notamment, que c'est bien la solution la plus juste qui a été retenue. Le considérant 84 du RGPD ne dit pas autre chose en affirmant qu'« il convient de tenir compte du résultat de cette analyse pour déterminer les mesures appropriées à prendre afin de démontrer que le traitement des données à caractère personnel respecte le présent règlement ».

Lorsque l'État met en place une nouvelle technologie qui va impacter les libertés citoyennes, il doit l'encadrer par une loi. C'est bien à ce stade-là que s'effectue le choix d'une technologie plutôt qu'une autre et la définition des différentes modalités qui l'entourent. C'est à ce stade-là que les députés, qui seront amenés à débattre de cette nouvelle mesure et notamment de sa proportionnalité, ont besoin d'être éclairés sur l'efficacité de la technologie envisagée, sur les mesures alternatives qui existent éventuellement, etc. C'est aussi grâce à cette analyse, que les responsables politiques pourront expliquer à la population la nécessité de recourir à telle technologie, et de les convaincre que tout a été mis en œuvre pour trouver la solution la plus équilibrée, avant d'ancrer cette solution dans une loi qui s'impose à tous.

Ainsi donc, une fois que le choix politique est fait, et bétonné dans une loi au terme d'un long processus législatif, la technologie sera mise en place telle quelle, au risque de ne pas respecter la loi. On voit donc difficilement comment une analyse d'impact qui serait effectuée beaucoup plus tard, au stade de la mise en œuvre effective de la technologie telle que décidée et encadrée par le législateur, pourrait modifier quoi que ce soit, si ce n'est en démontrant la nécessité de modifier la loi si on se rendait compte à ce stade de la disproportion de l'outil…

En somme, la raison d'être de l'analyse d'impact étant d'aider le responsable du traitement à choisir la technologie la plus adéquate, cette raison d'être se traduit par l'obligation, pour le législateur, d'effectuer cette analyse d'impact au moment de l'élaboration de la disposition destinée à l'encadrer, au risque de faire preuve d'une certaine mauvaise foi, voire d'un peu de cynisme dans la gestion des données de citoyens…

B. La pertinence de la mesure

17. Une mesure pertinente selon la Cour. Ainsi qu'on l'a dit, l'analyse de la pertinence de la mesure est la première étape de l'examen de proportionnalité de celle-ci. Il s'agit de s'assurer que la mesure est de nature à atteindre l'objectif poursuivi.

La Cour juge que l'insertion des empreintes digitales sur l'e-*id.* est une mesure pertinente, au motif que cette mesure est susceptible « de réduire le risque de falsification des cartes d'identité » et « de prévenir l'utilisation frauduleuse des cartes d'identité ».

vie privée. Légalité, transparence et contrôle, coll. Crids, Bruxelles, Larcier, 2014, n^os^ 102 et s.).

47 Cour const., arrêt n° 2/2021 du 14 janvier 2021 précité, B.7.4, dernier alinéa.

On ne perçoit pas ce qui convainc la Cour de la pertinence de la mesure. On constate par contre certaines hésitations, la Cour reconnaissant « l'absence de fiabilité totale du procédé et l'impossibilité corrélative d'exclure complètement la non-détection de certains cas de fraude à la ressemblance »[48]. Néanmoins, selon la Cour qui cite l'extrait d'un arrêt de la Cour de justice de l'Union européenne, il suffit que la mesure « réduise considérablement le risque (…) d'acceptations de personnes non autorisées » pour qu'on la considère pertinente.

La Cour admet donc qu'une mesure sévère – puisqu'il s'agit d'obliger toute la population à faire enregistrer ses empreintes digitales sur son e-*id*. – peut être pertinente alors qu'elle n'atteint pas pleinement son objectif puisqu'en l'occurrence, le risque existe que même l'enregistrement des empreintes digitales de toute la population ne permettra pas d'arrêter une personne qui se prévaut pourtant d'un document falsifié.

18. Des questions en suspens. À nouveau, on regrette l'absence d'analyse d'impact qui permettrait de comprendre les éléments techniques et le retour d'expérience, notamment, qui fondent les différentes affirmations de la Cour. Que signifie le fait de « réduire considérablement le risque » ? Quelle est la base de ce constat ? Des statistiques ont-elles été menées ? Quelles sont les causes de ce manque de fiabilité et comment résorber ces failles ? Les questions restent en suspens…

Par ailleurs, qu'en est-il de l'hypothèse inverse ? D'une personne qui serait arrêtée, alors même qu'elle ne détiendrait pas de document falsifié mais qu'un « bug » technique conduirait à considérer que les empreintes de ses doigts ne correspondent pas aux empreintes enregistrées sur la carte[49] ?

La Cour n'aborde pas ce risque, pourtant lié au fait que, comme l'ont soutenu les requérants, les empreintes digitales ne sont pas infaillibles.

C. La nécessité et la proportionnalité au sens strict de la mesure

19. La recherche de mesures alternatives. Après avoir analysé la pertinence de la mesure, la Cour examine ensuite la nécessité et la proportionnalité au sens strict de la mesure. Elle affirme qu'il y a lieu « de vérifier si l'ingérence ne va pas au-delà de ce qui est nécessaire à la réalisation des objectifs poursuivis et, en particulier, s'il existe des mesures qui sont moins attentatoires aux droits concernés, tout en contribuant de manière efficace au but de la réglementation en cause »[50].

Toutefois, il ressort des longs développements à ce sujet que ce n'est pas tant la recherche de mesures alternatives qui retient l'attention de la Cour, que de savoir s'il existe une analogie entre la carte d'identité nationale et le passeport européen. Puisque les empreintes digitales sont enregistrées sur le passeport, par

48 Cour const., arrêt n° 2/2021 du 14 janvier 2021 précité, B.21.1, alinéa 2.

49 Ce cas de figure a d'ailleurs fait la une de l'actualité il y a quelques temps, dans l'affaire *Dupond de Ligonnès*, qui défraie la chronique depuis de nombreuses années. À la recherche de ce père de famille qui a assassiné sa famille et reste introuvable à ce jour, la police de Glasgow a annoncé, en 2019, avoir retrouvé Monsieur Dupond de Ligonnès lors de son passage à l'aéroport de Glasgow. On affirmait alors qu'il aurait changé d'apparence physique mais que, grâce à un contrôle au départ des empreintes digitales, on avait pu le retrouver. L'histoire a montré qu'il n'en était rien. La correspondance entre les empreintes de ce voyageur et celles de Monsieur de Ligonnès était le fruit d'une erreur, l'utilisation des empreintes digitales n'étant pas infaillible. Voy. not. https://www.cnews.fr/france/2019-10-12/affaire-xavier-dupont-de-ligonnes-pourquoi-les-empreintes-digitales-peuvent-etre.

50 Cour const., arrêt n° 2/2021 du 14 janvier 2021 précité, B.25.2.

analogie, doit-il en être de même pour la carte d'identité ?

20. L'analogie avec le passeport. Le passeport est un document de voyage. Selon la Cour, la carte d'identité l'est aussi. Étant donné que les empreintes digitales sont enregistrées sur le passeport pour sécuriser ce document de voyage, la Cour estime qu'il devrait en être de même pour sécuriser la carte d'identité en tant que document de voyage.

La Cour fonde cette assimilation sur une pratique, relatée dans les travaux préparatoires, à savoir le fait que « les cartes d'identité sont aujourd'hui fréquemment utilisées comme documents de voyage au sein de l'Union européenne, ainsi que dans le cadre de voyages vers un nombre limité d'États tiers et qu'elles sont, à ce titre, susceptibles de faire l'objet de contrôles »[51]. La Cour se fonde également sur le règlement européen 2019/1157 précité qui impose des normes de sécurité et, notamment, l'enregistrement des empreintes digitales, tant pour les passeports que pour les cartes d'identité. Ce règlement est, pour rappel, applicable en Belgique depuis le 2 août 2021.

Pourtant, l'analogie entre passeport et carte d'identité n'est pas si évidente, tant d'un point de vue juridique que pratique. C'est la raison pour laquelle d'ailleurs les requérants avaient demandé à la Cour de poser une question préjudicielle à la Cour de justice de l'Union européenne à propos de la conformité de ce règlement aux exigences de protection de la vie privée et des données à caractère personnel[52]. Malheureusement, cette question préjudicielle n'a pas été posée.

Au niveau juridique, la finalité de l'e-*id.* ne peut être induite de ce qui se fait *de facto,* en pratique. Cette finalité doit être circonscrite par le législateur, ce qui a été fait dans la loi qui encadre l'e-*id.*, à savoir la loi du 19 juillet 1991. Celle-ci affirme, en son article 6, que la carte d'identité vaut certificat d'inscription dans les registres de la population. En d'autres termes, à la lecture de la loi, l'e-*id.* a donc pour unique finalité de servir de preuve d'inscription aux registres de la population. L'arrêté royal du 25 mars 2003 – et bien qu'il eût fallu que ce soit précisé dans la loi – ajoute qu'elle sert à établir l'identité d'une personne[53]. Elle doit ainsi être présentée à toute réquisition de la police, ainsi qu'à l'occasion de toute déclaration, toute demande de certificats et, « d'une manière générale, lorsqu'il s'agit d'établir l'identité du porteur »[54].

Il n'entre donc pas dans les finalités légales de l'e-*id.* d'être un document de voyage, du moins tant que le législateur belge ne l'a pas prévu explicitement dans la loi encadrant l'e-*id.* On peut d'ailleurs se demander s'il serait opportun et nécessaire de faire de l'e-*id.* un document de voyage. En effet, les citoyens européens bénéficient de la liberté de circulation au sein de l'Union européenne et certains pays tiers, ce qui explique qu'ils peuvent voyager sans être systématiquement contrôlés. Dès lors, si l'on considère que l'e-*id.* est un document de voyage comme le passeport et qu'elle doit contenir les mêmes données, ne prend-on pas le risque de raisonner au départ d'un postulat bancal ? Il ne faudrait pas que le fait d'affirmer que l'e-*id.* est nécessaire pour voyager en Europe porte atteinte à la liberté de circulation en Europe. Il ne faudrait pas non plus qu'estimer que l'e-*id.* serait nécessaire pour voyager hors Europe, aboutisse à ce que l'e-*id.* fasse double emploi avec le passeport.

Dans le même sens, dans l'avis rendu à propos de la proposition de règlement devenue le

51 *Ibid.*, B. 26.4.

52 *Ibid.*, A.35.1.

53 Arrêté royal du 25 mars 2003 relatif aux cartes d'identité, *op. cit.*, articles 1 et 3, § 1, al. 1.

54 *Ibid.*, article 1, al. 2.

règlement européen 2019/1157 précité, le Comité européen de la protection des données a affirmé mettre « en doute la valeur ajoutée de l'intégration des données biométriques dans les cartes d'identité, étant donné qu'elles ne sont pas systématiquement contrôlées lors des voyages entre États membres de l'Union »[55]. L'Autorité de protection des données s'est prononcée en ce sens également[56].

Outre ces considérations juridiques, le passeport et la carte d'identité peuvent également être distingués sur le plan pratique. Comme l'indique le Comité européen de protection des données, « les cartes d'identité font l'objet de diverses utilisations qui vont bien au-delà de l'exercice du droit à la libre circulation lié à la citoyenneté de l'Union, depuis les démarches auprès des administrations du pays d'origine du citoyen jusqu'aux relations avec différents acteurs du secteur privé (banques, compagnies aériennes, etc.) »[57], comme l'a confirmé l'Autorité de protection des données elle aussi[58]. C'est particulièrement vrai en Belgique, où la carte d'identité est même utilisée comme carte de fidélité dans certains magasins.

Heureusement, les utilisations multiples de l'e-*id.* ont retenu l'attention de la Cour, comme on l'explique au point suivant.

21. Les particularités de l'e-*id*. Tout en soutenant qu'« une analogie entre les passeports et les cartes d'identité est donc permise »[59], la Cour affirme qu'« il peut être admis, avec le CEPD et l'Autorité de protection des données, que le test de nécessité et de proportionnalité doit être plus strict pour les passeports, compte tenu notamment de l'importance des premières dans les actes de la vie quotidienne et du caractère obligatoire de leur détention », si bien qu'« il incombe donc à la Cour de vérifier si, en l'espèce, le législateur a pris une mesure qui est nécessaire et proportionnée à l'objectif poursuivi »[60].

La Cour se livre donc à une analyse entre le(s) avantage(s) de la mesure et le(s) inconvénient(s) qu'elle crée.

22. Les avantages de l'enregistrement des empreintes digitales sur l'e-*id*. Pour la Cour, la mesure vise à lutter contre une fraude qui n'est pas « purement marginale »[61]. Elle reconnaît que « les chiffres relatifs à la fraude documentaire ont diminué » mais pas « les chiffres relatifs à la fraude à la ressemblance, ces chiffres visant par ailleurs uniquement les fraudes détectées »[62].

Ainsi donc, la Cour admet qu'il s'agit en définitive d'agir principalement contre la seule fraude à la ressemblance. Elle se fonde sur des affirmations figurant dans les travaux préparatoires de la loi, qui ne coïncident pourtant pas avec les chiffres avancés tant par le Comité européen de protection des données que par l'Autorité de protection des données[63].

23. Les mesures alternatives existantes. Est-il alors nécessaire d'enregistrer les empreintes digitales de toute la population, pour lutter principalement contre la fraude à

55 Comité européen de la protection des données, avis n° 7/2018 du 10 août 2018, sur la proposition de règlement relatif au renforcement de la sécurité des cartes d'identité des citoyens de l'Union et d'autres documents, p. 11, n° 22.

56 Autorité de protection des données, avis n° 106/2018 du 17 octobre 2018, n° 25.

57 Comité européen de la protection des données, avis n° 7/2018 du 10 août 2018, sur la proposition de règlement relatif au renforcement de la sécurité des cartes d'identité des citoyens de l'Union et d'autres documents, p. 11, n° 23.

58 Autorité de protection des données, avis n° 106/2018 du 17 octobre 2018, n° 25.

59 Cour const., arrêt n° 2/2021 du 14 janvier 2021 précité, B. 26.5.

60 *Ibid.*, B.26.5.

61 *Ibid.*, B.28.

62 *Ibid.*, B.28.

63 Autorité de protection des données, avis n° 106/2018 du 17 octobre 2018, n° 24.

la ressemblance dont l'ampleur est discutée ? Fraude qui est le fait des individus qui sont parvenus à obtenir une carte d'identité volée ou perdue, à ressembler à la photo figurant sur cette carte et à passer outre les contraintes techniques déjà en place, comme le blocage des cartes dont la perte ou le vol a été signalé ? N'existe-t-il pas de solution alternative qui ne requiert pas l'enregistrement de nouvelles données ni n'impacte tous les citoyens ?

C'est la question posée par les requérants, soulignant le caractère suffisant d'un autre élément biométrique présent sur l'e-*id.*, à savoir la photo, éventuellement conjugué à des mesures moins intrusives de vérification de l'authenticité de la carte[64]. Et de soutenir que « l'administration peut consulter la photographie qui figure sur la carte d'identité pendant quinze ans, ce qui rend impossible la fraude consistant à obtenir des documents authentiques sur la base de documents faux ou volés. L'administration étant immédiatement informée de la perte ou du vol d'une carte d'identité, compte tenu de l'obligation pour le citoyen de signaler cette perte ou ce vol, elle peut bloquer aussitôt les certificats de sécurité de la carte. Ensuite, la probabilité que deux personnes se ressemblent au point qu'une confusion soit possible est très faible »[65].

Malheureusement, et bien que ce fut une belle occasion de s'assurer de l'existence, ou non, de mesure alternative, la Cour ne dit rien, ni au sujet de la photo ni par rapport aux autres mesures techniques envisagées par les requérants.

24. Les risques de la mesure. La Cour se concentre sur l'existence de risques éventuels liés à l'enregistrement des empreintes digitales sur l'e-*id.* On se concentre ici sur le risque d'un enregistrement centralisé des données, pointé par les requérants[66].

La Cour constate que « la disposition attaquée n'établit pas un registre central des empreintes digitales de l'ensemble des détenteurs d'une carte d'identité »[67]. Elle nuance immédiatement cette affirmation en rappelant que les empreintes digitales sont conservées « pour les besoins de la fabrication et de la délivrance de la carte d'identité, pendant une durée maximale de trois mois ».

En d'autres termes, il existe déjà une « base de données centralisée »[68] qui enregistre les empreintes digitales pendant une période pouvant aller jusqu'à trois mois.

D'une part, du seul fait de l'enregistrement de ces données, *a fortiori* pendant trois mois, des risques existent. Il peut s'agir d'un piratage externe ou d'un abus de données émanant d'une personne ayant accès à cette base de données.

D'autre part, peut-on exclure le risque d'une centralisation des données à plus long terme, comme semble le penser la Cour ? Rien ne permet de le dire. La centralisation des données et leur durée maximale sont fixées dans une loi. Il faudrait donc, en principe[69], une modification législative pour étendre cette durée. Quand bien même cette modification se

64 Les requérants citent les techniques de « Sensor on card » et de « Match on card ». Voy. Cour const., arrêt n° 2/2021 du 14 janvier 2021 précité, A.18.2.1.

65 Cour const., arrêt n° 2/2021 du 14 janvier 2021 précité, A. 16.3.

66 *Ibid.*, A.18.2.1. Les risques liés à la centralisation de ces données ont été analysés par des chercheurs de la KULeuven dans l'étude suivante : J. Hermans et R. Peeters, « Vingerafdrukken op de Belgische eID Technische analyse », s.d., accessible ici https://www.esat.kuleuven.be/cosic/publications/article-3004.pdf.

67 Cour const., arrêt n° 2/2021 du 14 janvier 2021 précité, B.31.1.

68 Voy. également Cour const., arrêt n° 2/2021 du 14 janvier 2021 précité, B.38.1 qui utilise expressément ce terme.

69 La pandémie, notamment, et avant elle, la mise en place de certains dispositifs de traitements de données par l'État, ont montré que le principe de légalité n'est pas toujours respecté en pratique…

ferait par une loi, on pourrait ne pas percevoir clairement ni l'existence ni la portée de pareille modification.

En guise d'exemple récent, l'avant-projet de loi « Pandémie »[70] comprenait, dans sa version initiale, un article 6 déléguant au Roi la possibilité de réutiliser des bases données pour d'autres finalités que celles prévues par la loi ayant créé ladite base de données. Si cette disposition avait été adoptée, elle aurait permis de réutiliser à d'autres fins et pour une période non définie, les données enregistrées dans la base de données « empreintes digitales ».

C'est la raison pour laquelle il ne faut pas ignorer que la création d'une base de données constitue en elle-même un risque, et justifie qu'on en appelle à une particulière prudence dans ce domaine.

25. Un risque à plus long terme. Au-delà des risques soulevés par les requérants et les réponses apportées par la Cour, on s'interroge sur le rôle et l'évolution, à plus long terme, de l'e-*id.*

Ainsi que nous l'avons déjà montré dans une précédente contribution[71], le citoyen n'a pas le choix : il est contraint de détenir une e-*id.* personnelle, et d'accepter qu'y soient placées certaines données. Or, l'enregistrement des empreintes digitales montre que ces données sont de plus en plus nombreuses sans que leur nécessité n'apparaisse clairement. Par ailleurs, les usages de l'e-*id.* se diversifient, jusqu'à être utilisée dans le secteur privé, comme carte de fidélité par exemple.

Ne doit-on pas y voir une tendance à banaliser l'usage de l'e-*id.* qui pourrait aboutir à en faire, dans un futur pas si lointain, un « pass » pour citoyen ? De preuve d'inscription dans les registres de la population, hier, il devient aujourd'hui, à la faveur de l'interprétation qu'en fait la Cour constitutionnelle notamment, et sans que le législateur l'ait décidé et inscrit dans une loi, un document de voyage pour franchir les frontières européennes. Demain, l'e-*id.* accueillera-t-elle les « pass » permettant de filtrer les personnes pouvant accéder aux restaurants, aux théâtres, aux concerts en fonction de leur état de santé ou de leur passé judiciaire ?

La question mérite d'être posée. Récemment, le gouvernement belge a décidé, seul, et sans débat démocratique, de limiter l'accès à certains lieux et services aux personnes qui peuvent se prévaloir d'un « pass », initialement appelé « coronapass », rebaptisé aujourd'hui « Covid safety ticket ».

Ce « pass » pose question sur le fond. Aujourd'hui utilisé pour le Covid, il pourrait demain servir à limiter l'accès à certains lieux, services ou produits, aux personnes qui présentent d'autres maladies voire, un autre risque. On songe par exemple aux personnes suspectées de harcèlement ou de terrorisme et qui présentent un risque pour la sécurité physique des autres citoyens.

Sur la forme, se pose la question du format de ce « pass ». Actuellement, il est envisagé que celui-ci prenne la forme d'un QR code placé sur un smartphone. Or, concrètement, cela risque de poser problème puisque certaines personnes ne disposent pas d'un smartphone. En outre, comment contrôler que la personne présentant un QR code sur smartphone affirmant par exemple que la personne est vaccinée, est bien le propriétaire de ce smartphone et non quelqu'un qui aurait emprunté le smartphone d'une personne vaccinée pour passer le contrôle ?

[70] Avant-projet de loi relative aux mesures de police administrative lors d'une situation d'urgence épidémique, daté du 26 février 2021.

[71] E. Degrave et J. Mont, « La carte d'identité électronique à la lumière du droit à la protection de la vie privée », *op. cit.*, pp. 3-15.

Pour contourner ce type de problème, il pourrait être tentant, pour certains, de placer les résultats médicaux sur la puce de l'e-*id.*, puisque chacun est obligé de disposer d'une e-*id.* Celle-ci n'aurait plus qu'à être scannée par le lecteur *ad hoc* au moment de vérifier l'état de santé des personnes prétendant aller au concert, par exemple… D'aucuns verraient là un moyen de contourner le problème de la fracture numérique et du contrôle d'identité…

Or, plus l'e-*id.* contiendra de données, plus on pourra surveiller et contrôler les individus au départ de cette petite carte en en étendant les usages, toujours pour « la bonne cause ». Par exemple, et pour en revenir à la question des empreintes digitales sur l'e-*id.*, pour lutter contre un risque terroriste, le gouvernement pourrait estimer utile d'empêcher l'accès des personnes fichées par la police à certains lieux publics, comme une salle de concert. Les empreintes digitales étant enregistrées à la fois sur l'e-*id.* et dans les fichiers de la police, on ne peut pas exclure que, par souci d'efficacité toujours, soit organisée la confrontation entre la puce de l'e-*id.* et le fichier de la police, pour écarter les personnes considérées comme peu fiables.

Ce serait là s'engouffrer dans un dangereux engrenage. D'outil d'identification, l'e-*id.* deviendrait un outil de sélection voire d'exclusion de certains citoyens. Alors que, depuis les Lumières, les libertés citoyennes sont définies de manière générale et abstraite dans la loi par souci d'égalité entre tous les citoyens, leur exercice effectif serait désormais conditionné à la présentation d'une e-*id.* délimitant, au cas par cas, les libertés auxquelles chaque citoyen peut prétendre en fonction de son profil personnel, de santé ou judiciaire, notamment. Profil qui sera contrôlé par des acteurs privés (restaurateurs, sorteurs de boîtes de nuit, personnel des salles de théâtre et de concert, …) qui ne sont pas habilités pour ce faire et ne sont eux-mêmes pas demandeurs de ce rôle de « douaniers ». Le tout sans garantie que ce qui constituera un vrai choix de société n'ait été véritablement discuté et décidé au terme d'un débat démocratique éclairé, éclairant, et assumé politiquement.

V. CONCLUSION

Lutter contre la fraude à l'identité est certes un objectif louable dans une société démocratique. Néanmoins, imposer à chaque citoyen que ses empreintes digitales soient enregistrées sur l'e-*id.* qu'il est obligé de détenir n'est pas une mesure anodine. Elle touche à la vie privée de tous les citoyens, mais également à d'autres de leurs libertés importantes comme la liberté d'aller et venir, la liberté de se rassembler, la liberté de travailler, dès lors que le législateur belge et la Cour constitutionnelle envisagent l'e-*id.* comme un document de voyage qui sert à contrôler les individus lors de leurs déplacements.

L'arrêt de la Cour constitutionnelle laisse perplexe. La Cour se prononce sur la pertinence et la nécessité de la mesure sans qu'une analyse d'impact n'ait été réalisée et alors même que les chiffres de fraude avancés par le législateur et les requérants divergent. Dans le même temps, elle reconnaît « l'absence de fiabilité totale du procédé » et « l'impossibilité corrélative d'exclure complètement la non-détection de certains cas de fraude »[72]. Au final, on peine à comprendre en quoi cette mesure est pertinente et nécessaire, alors même qu'il s'agit ici de s'assurer, comme le rappelle la Cour, qu'elle répond à un « besoin social impérieux »[73].

On regrette également que l'analyse des risques de cette technologie se concentre essentiellement sur l'analogie très discutable

[72] Cour const., arrêt n° 2/2021 du 14 janvier 2021 précité, B.21.1.

[73] *Ibid.*, B.14.2.

entre passeport et e-*id.*, alors même que celle-ci a été vivement critiquée par deux autorités distinctes, l'Autorité de protection des données, en Belgique, et le Comité européen de protection des données, et que les requérants demandaient de poser une intéressante question préjudicielle à la CJUE.

En définitive, il s'agit là d'une occasion manquée d'analyser les mesures alternatives possibles et d'envisager l'ensemble des risques, ce qui est pourtant particulièrement important à l'heure où recourir aux technologies apparaît de plus en plus souvent comme une « baguette magique » pour nombre de problèmes, au risque d'ignorer un impact non négligeable de ces outils à moyen et long terme. C'est le cas en l'espèce. On peut raisonnablement s'inquiéter de la banalisation de l'e-*id.* qui consiste notamment à lui donner un rôle qui n'a pas été défini dans la loi, comme le montre encore cet arrêt en assimilant l'e-*id.* à un document de voyage sur la base de constats principalement factuels.

Les données qui sont inscrites sur l'e-*id.* subissent également cette même banalisation. Aujourd'hui enregistrées pour lutter contre la fraude à l'identité, pour quelles fins seront utilisées les empreintes digitales demain ? L'enthousiasme de certains autour de la mise en place d'un « coronapass », rebaptisé « covid safety ticket », en dehors de tout cadre légal, doit nous alerter sur une possible « société du pass » naissante, qui risque de conditionner les libertés au respect d'un profil jugé sécurisé, et dont l'e-*id.* sera le précieux sésame pour ouvrir la porte des restaurants, des théâtres, des concerts aux personnes qui pourront se prévaloir d'un « risque zéro » sur le plan sanitaire et peut-être judiciaire.

Est-ce de cette société-là que nous voulons ? Une grande question à laquelle ne cesseront de nous renvoyer les évolutions de cette toute petite carte…

Elise Degrave et Julie Mont