

La carte d'identité électronique à la lumière du droit à la protection de la vie privée

Elise DEGRAVE

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

Julie MONT

Assistante à la Faculté de droit de l'UNamur, Chercheuse au Nadi/Crids et Avocate au barreau de Namur

TABLE DES MATIÈRES

Prélude	3
I. L'importance de la loi pour encadrer un choix technologique imposé aux citoyens	4
II. Quelle est la raison d'être de l'e-id ?	5
III. Que contient l'e-id ?	5
A. Le prélèvement et la conservation de l'image numérisée des empreintes sur l'e-id	8
B. La conservation de l'image des empreintes pendant la fabrication et la délivrance de la carte	8
C. La lecture de l'image des empreintes digitales par les instances habilitées à cet effet	9
IV. Quelles utilisations peut-on faire l'e-id ?	9
A. L'autorité ou la personne qui utilise l'e-id d'un citoyen	9
B. Le type de données traitées	11
C. Le type de traitement effectué	13
Conclusion	14

Prélude

1. Un outil méconnu – S'il est un document administratif que chacun emporte tous les jours avec lui, c'est la carte d'identité électronique (ci-après, « e-id »). Pourtant, rares sont les citoyens qui savent ce qui est enregistré sur cette carte, et ce à quoi elle peut servir.

L'e-id concentre quantité de données à caractère personnel et génère de multiples traitements de ces données. A ce titre, ce document soulève maints enjeux en termes de protection de la vie privée et notamment, de compréhension, par chaque citoyen, de ce qui peut être fait de quelle donnée.

C'est donc à la croisée entre le droit administratif et le droit du numérique que se déclinent nos réflexions.

2. Du papier à l'électronique – Suite à la Première Guerre mondiale, l'obligation de disposer d'une carte

d'identité a été imposée aux Belges à partir de l'âge de quinze ans. La délivrance de ce document d'identité avait pour objectif d'associer la tenue des registres de population communaux à des recensements décennaux pour déterminer le chiffre annuel de population entre deux recensements¹. Outre cette finalité de recensement, la fonction principale de la carte d'identité papier était d'assurer l'identification de son titulaire.

La Belgique, soucieuse de s'inscrire dans l'évolution technologique et de développer l'administration électronique (aussi appelée « e-gouvernement »), s'est révélée être un pays précurseur², en 2003, lorsque la carte d'identité électronique a été créée³.

Au fil des années et des modifications législatives, les données qui figurent sur l'e-id, qu'elles soient visibles ou intégrées sur la puce, ont évolué.

Aujourd'hui et comme nous le verrons dans la suite du propos⁴, l'e-id comporte un nombre important de données à caractère personnel et fait l'objet d'usages divers et variés.

Si la simple lecture visuelle de la carte ne constitue pas un traitement de données, lorsque l'e-id est lue suivant un procédé automatisé ou que les données qui y sont contenues font l'objet d'un enregistrement dans un fichier, l'e-id fait l'objet de traitements de données. C'est par exemple le cas lorsqu'elle est présentée pour obtenir un service public (ex. : commander un extrait de casier judiciaire sur le site de son administration communale) ou un service privé (ex. : ouvrir un compte bancaire auprès d'une banque). Nous verrons, dans la suite de cette étude, que ces traitements sont soumis à un régime juridique *ad hoc*.

Comme nous aurons également l'occasion de l'indiquer ci-après, la multiplication tant des données

1. Projet de loi du 13 décembre 1990 relatif aux registres de population et aux cartes d'identité, Exposé des motifs, *Doc.*, Sénat, 1990-1991, n° 1150-1, p. 1.
 2. La Belgique suit de près la Finlande, premier pays à avoir déployé une carte d'identité électronique, en 1999. Le Règlement européen 2019/1157 du 20 juin 2019 (*J.O.U.E.*, 12 juillet 2019), qui sera applicable en août 2021 prévoit la mise en place d'une carte d'identité électronique à l'échelle de tous les pays européens.
 3. Projet de loi du 15 janvier 2003 modifiant la loi du 8 août 1983 organisant un Registre national des personnes physiques et la loi du 19 juillet 1991 relative aux registres de la population et aux cartes d'identité et modifiant la loi du 8 août 1983 organisant un registre national des personnes physiques, *Doc. parl.*, Chambre, sess. 2002-2003, 2226/001, p. 23.
 4. Cf. *infra*, n° 9 et n° 10.

figurant sur l'e-id que des usages qui en sont faits proviennent d'une succession et d'une accumulation de normes, de valeur législative et réglementaire, ayant souvent fait l'objet de plusieurs modifications⁵. Ce corps de règles est peu clair et engendre souvent un manque de transparence vis-à-vis des citoyens qui sont peu ou mal informés. Ceux-ci peuvent en conséquence perdre le contrôle sur cet outil d'identité, dont la légalité devient alors douteuse.

I. L'importance de la loi pour encadrer un choix technologique imposé aux citoyens

3. La légalité de l'e-id aux confins du RGPD, de la C.E.D.H. et de la Constitution – Ainsi qu'on l'a dit, l'e-id contient nombre de données à caractère personnel et génère de multiples traitements de celles-ci (collecte des informations, enregistrement de celles-ci, réutilisations ultérieures des données à l'occasion de l'usage de l'e-id, etc.). C'est un outil technologique dont les usages multiples ont des conséquences sur la vie des citoyens, notamment leur vie privée.

Pour cette raison, l'e-id doit être légalement et précisément encadrée, en respectant, d'une part, le Règlement Général pour la Protection des données à caractère personnel (ci-après, « RGPD »), et, d'autre part, les exigences de l'article 8 de la Convention européenne des droits de l'homme (ci-après, « C.E.D.H. ») et de l'article 22 de la Constitution qui encadrent les ingérences dans le droit à la vie privée. Ces normes fixent des exigences claires s'agissant de la légalité d'un outil comme l'e-id.

Ainsi, en vertu de l'article 6.1., c), du RGPD, l'e-id doit être « nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis »⁶.

Cette disposition doit être lue conjointement avec l'article 8 C.E.D.H. et l'article 22 de la Constitution⁷ qui, tous deux, affirment que toute ingérence dans la vie privée – telle que l'utilisation de données à caractère personnel – doit être organisée par une loi. A la

lumière de la jurisprudence de la Cour européenne des droits de l'homme et de la Cour constitutionnelle ainsi que de la jurisprudence de la Section de législation du Conseil d'Etat, il doit s'agir de dispositions claires et précises, permettant à chacun de prévoir ce qu'il va advenir de ses données une fois qu'il les aura communiquées. Par ailleurs, il doit s'agir d'une norme de valeur législative émanant d'un pouvoir législatif – et non d'une norme de valeur réglementaire émanant du pouvoir exécutif – étant donné que toute ingérence dans la vie privée des citoyens doit se faire au terme d'un débat démocratique qui se penche notamment sur la recherche de l'équilibre entre l'objectif d'efficacité administrative et les moyens numériques mis en place pour y arriver. Certes, en matière de numérique, la tentation est grande de faire confiance aux techniciens qui proposent un outil technique qui semble efficace et de « bricoler » un texte autour de cet outil. Ce serait là, admettre que la technologie fait loi. Un outil technologique mis en place par l'Etat pour les citoyens impacte la vie quotidienne de ces citoyens. Le choix technologique est donc un choix de société. Ce choix de société doit être débattu et décidé au sein d'un Parlement et non dans l'ombre des laboratoires de techniciens.

Plus précisément, cela signifie qu'une loi claire et précise, adoptée au terme d'un débat démocratique, doit déterminer les « éléments essentiels »⁸ du traitement de données envisagé. Il s'agit notamment de la raison d'être du traitement (appelé « finalité du traitement »), des données utilisées et des types de réutilisation de données⁹.

4. Plan – La présente étude confronte l'e-id à ces différentes exigences légales, au travers de l'analyse de trois questions clé.

Tout d'abord, quelle est la *raison d'être* de l'e-id ? Dans l'univers du droit du numérique, cela revient à analyser les « finalités » de l'e-id.

Ensuite, que *contient* l'e-id ? Il s'agit de s'interroger sur les données à caractère personnel qui sont intégrées à la e-id et d'examiner la proportionnalité de celles-ci.

5. 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 ; loi du 25 mars 2003 modifiant la loi du 8 août 1983 organisant un registre national des personnes physiques et la loi du 19 juillet 1991 relative aux registres de la population et aux cartes d'identité et modifiant la loi du 8 août 1983 organisant un registre national des personnes physiques, *M.B.*, 28 mars 2003 ; arrêté royal du 25 mars 2003 relatif aux cartes d'identité, *M.B.*, 28 mars 2003 ; loi du 25 novembre 2018 portant des dispositions diverses concernant le Registre national et les registres de population, *M.B.*, 13 décembre 2018 ; loi du 18 juin 2020 modifiant la 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.*, 30 juin 2020.

6. Une autre base juridique dans le RGPD pourrait être l'article 6.3 du RGPD. Le gouvernement a toutefois récemment précisé qu'il s'agissait de l'article 6.1., c), dans la mesure où il s'agissait d'exécuter les obligations prévues par la loi du 19 juillet 1991 sur les registres de la population, sur laquelle nous reviendrons ultérieurement (Rapport au Roi précédant l'arrêté royal du 10 décembre 2019 modifiant l'arrêté royal du 25 mars 2003 relatif aux cartes d'identité et l'arrêté royal du 19 avril 2014 relatif aux cartes d'identité délivrées par les postes consulaires de carrière, *M.B.*, 20 décembre 2019).

7. Autorité de protection des données (ci-après « APD »), avis n° 100/2019 du 3 avril 2019 relatif à un projet d'arrêté royal modifiant l'arrêté royal du 25 mars 2003 relatif aux cartes d'identité (CO-A-2019-087), n° 3.

8. Voir not. C.C., arrêt n° 202/2004, *op. cit.*, B.6.2. et B.6.3.

9. Pour de plus amples informations à ce sujet, voir E. DEGRAVE, *Le-gouvernement et la protection de la vie privée. Légalité, transparence et contrôle*, Bruxelles, Larcier, 2014, pp. 163 et s. et références citées. L'APD abonde dans le même sens dans plusieurs avis au sujet de traitements de données dans le secteur public (voir not APD, avis n° 100/2019 précité ; APD, avis n° 64/2020 du 20 juillet 2020 concernant un projet d'accord de coopération (...) dans le cadre d'un suivi des contacts auprès des personnes (présümées) infectées par le coronavirus COVID-19 sur la base d'une base de données auprès de Sciensano (CO-A2020-076)).

Enfin, quels sont les *usages* de l'e-id légalement autorisés ? Le citoyen peut-il contrôler ceux-ci ?

II. Quelle est la raison d'être de l'e-id ?

5. La finalité du traitement de données – Identifier la raison d'être de l'e-id consiste à circonscrire les finalités poursuivies par la collecte, l'enregistrement et la réutilisation des données qui se trouvent sur l'e-id. En d'autres termes, pour quelle(s) raison(s) le législateur a-t-il créé la carte d'identité – d'abord en format papier, puis en format numérique – et a-t-il décidé d'y intégrer nombre de données à caractère personnel ?

Cette question est essentielle. En effet, la finalité d'un traitement de données est « la clé de voûte »¹⁰ de celui-ci. En l'occurrence, c'est en fonction des finalités de l'e-id que l'on peut examiner la pertinence et la nécessité d'enregistrer tant de données sur l'e-id et de diversifier ses usages.

6. Détermination claire dans la loi – Ainsi qu'on l'a dit précédemment, la finalité est un élément essentiel d'un traitement de données. Conformément à la jurisprudence des hautes juridictions, elle doit donc être déterminée de manière claire et précise dans la loi, pour que chacun puisse, à la lecture de la loi, comprendre les raisons qui sous-tendent la création et l'utilisation de l'e-id.

7. Les finalités légales de l'e-id – Que prévoit la loi en l'espèce ?

L'article 6 de la loi du 19 juillet 1991 prévoit que la carte d'identité vaut certificat d'inscription dans les registres de la population. A 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 ajoute qu'elle sert à *établir l'identité d'une personne*¹¹. 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 »¹². L'e-id permet, depuis 2003, d'identifier et d'authentifier une personne à distance de manière électronique.

Il est évident que c'est pour répondre à cet objectif principal que la carte d'identité existe. Mais excepté dans ces deux instruments normatifs – dont l'un n'est pas de valeur législative –, il est particulièrement fastidieux de trouver les motifs exacts qui ont amené

l'Etat à faire évoluer l'e-id et à y intégrer une multitude de données à caractère personnel.

C'est notamment le cas pour les données biométriques insérées sur l'e-id depuis 2018, et sur lesquelles nous reviendrons plus loin¹³. La loi n'explique pas les raisons pour lesquelles ces données figurent sur la carte, et ce sont les travaux préparatoires de celle-ci qui apprennent que le législateur a souhaité lutter contre la fraude à l'identité. Cette finalité est toutefois extrêmement fragile, notamment en l'absence de justification étayée et chiffrée de cas avérés de fraude, ainsi que l'avait d'ailleurs relevé l'APD lorsqu'elle s'était penchée sur le texte du projet de loi¹⁴.

Il est important de rappeler que le premier instrument législatif qui a légalisé de manière explicite la délivrance de la carte d'identité, soit la loi adoptée en juillet 1991, prévoyait que seules trois catégories de données figuraient sur la carte, soit les données d'identification spécifique à son titulaire, les titres des rubriques comprenant ces données et les mentions « carte d'identité » et « Belgique ». Le numéro d'identification au Registre national était mentionné sur la carte uniquement lorsque le titulaire en faisait la demande. Les auteurs du texte avaient en effet considéré que, dans la mesure où ce numéro pouvait entraîner des « intrusions » dans la vie privée du titulaire de la carte, celui-ci pouvait choisir de l'y inscrire (en réalité sur une vignette adhésive apposée au verso de la carte) ou non¹⁵.

Force est de constater que ces données étaient vraisemblablement suffisantes, en 1991, pour démontrer valablement son identité, finalité première de la carte d'identité.

Il est donc permis de s'interroger sur l'opportunité – alors que permettre de rapporter la preuve de son identité est la finalité principale de l'e-id – d'intégrer à cette carte toujours plus de nouvelles données, dont les finalités, outre le fait qu'elles soient peu claires et fragiles, ne sont parfois tout simplement pas précisées par le législateur.

III. Que contient l'e-id ?

8. Données proportionnées – De nombreuses données sont placées sur l'e-id. Selon le législateur, elles sont nécessaires pour atteindre les finalités évoquées précédemment.

10. Selon une expression désormais classique en matière de protection des données.

11. Arrêté royal du 25 mars 2003 relatif aux cartes d'identité, *M.B.*, 28 mars 2003, art. 1 et 3, § 1, al. 1.

12. Arrêté royal du 25 mars 2003 relatif aux cartes d'identité, *op. cit.*, art. 1, al. 2.

13. Cf. n° 10 ci-après.

14. APD, avis n° 19/2018 du 28 février 2018, n° 69.

15. Projet de loi du 13 décembre 1990 relatif aux registres de population et aux cartes d'identité, Commentaire des articles, *op. cit.*, p. 6.

Ce critère de nécessité fait partie de l'exigence de proportionnalité imposée par les articles 8 C.E.D.H. et 22 de la Constitution qui conditionnent chaque ingérence dans la vie privée, au fait que celle-ci soit nécessaire à la réalisation de l'objectif légitime poursuivi. Cette exigence est consacrée par le RGPD également, via le principe de « minimisation des données », selon lequel seules les données nécessaires à l'objectif poursuivi peuvent être traitées. En d'autres termes, dès qu'il est question de traiter des données, il y a lieu de s'assurer que ce traitement est, non seulement, pertinent pour atteindre l'objectif poursuivi (« collecter telle donnée va-t-il permettre d'atteindre tel objectif ? ») mais également nécessaire (« même si collecter telle donnée permet d'atteindre tel objectif, n'existe-t-il pas une alternative – consistant à ne pas collecter de données ou à en collecter moins – qui permettrait d'atteindre le même résultat, tout en créant moins de dégâts collatéraux pour la protection de la vie privée de chacun ? »).

A cet égard, la récente intégration des empreintes digitales sur l'e-id pose question au regard de l'exigence de proportionnalité et, en particulier, du critère de nécessité.

9. Données visibles et invisibles

Après avoir évolué au fil non seulement du temps mais également des modifications législatives, la liste des données figurant sur la carte d'identité se trouve dans la loi du 19 juillet 1991.

Elle se présente à ce jour comme suit¹⁶ :

1) *Les données visibles* :

- le nom ;
- les deux premiers prénoms et la première lettre du troisième prénom ;
- la nationalité ;
- le lieu et la date de naissance ;
- le sexe ;
- le lieu de délivrance de la carte ;
- la date de début et de fin de validité de la carte ;
- la dénomination et le numéro de la carte ;
- la photographie ;
- la signature ;
- la signature du fonctionnaire communal ;
- le numéro de registre national ;

- le lieu de naissance (uniquement pour les citoyens qui détiennent une carte délivrée avant l'entrée en vigueur de la loi du 18 juin 2020¹⁷).

2) *Les données invisibles* :

- toutes les données lisibles à l'œil nu, exceptées les signatures du titulaire et du fonctionnaire communal ;
- les clés d'identité et de signature ;
- les certificats d'identité et de signature ;
- le prestataire de service de certification accrédité ;
- l'information nécessaire à l'authentification de la carte et à la protection des données visibles de manière électronique ;
- la résidence principale (l'idée étant d'éviter d'inscrire de manière visible une « donnée très fluctuante » puisque chaque année, environ 10 % de la population change d'adresse¹⁸) ;
- le lieu de naissance (uniquement pour les citoyens qui détiennent une carte délivrée après l'entrée en vigueur de la loi du 18 juin 2020) ;
- la mention visée à l'article 374/1 du Code civil¹⁹ ;
- l'image numérisée des empreintes digitales de l'index de la main gauche et de la main droite du titulaire ou, en cas d'invalidité, d'un autre doigt de chaque main et le lieu de naissance ;
- les « autres mentions, prévues ou autorisées par la loi ainsi que les mentions imposées par la législation européenne ».

S'agissant de cette dernière catégorie, en vertu du principe de légalité, qui exige que la loi soit claire et suffisamment précise pour être prévisible pour les citoyens, il conviendrait que le législateur énonce l'ensemble de ces « autres mentions » susceptibles de figurer sur l'e-id dans une liste exhaustive. En guise d'exemple, les informations recueillies du SPF Affaires étrangères semblent indiquer que le titre de noble éventuel du citoyen figure sur la carte d'identité²⁰. Malgré des recherches, la base légale légitimant la présence de cette donnée n'a pas pu être identifiée.

A noter également que bien que non repris sur la liste de la loi du 19 juillet 1991, figure au rang des données invisibles présentes sur l'e-id un code-barres bidimensionnel qui comprend le numéro de Registre national, le numéro de carte, la durée de validité et la date de naissance. La présence de ce code-barres existait avant qu'une base légale le prévoie, puisque c'est sur la recommandation de l'APD que l'arrêté royal du

16. Loi du 19 juillet 1991, *op. cit.*, art. 6, § 2.

17. Loi du 18 juin 2020 modifiant la 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.*, 30 juin 2020.

18. *Ibid.*, p. 25.

19. Cet article a été inséré dans le Code civil par la loi du 22 mai 2014 visant à prévenir l'enlèvement parental international d'enfants. Concrètement, cette disposition autorise la personne qui s'est vue attribuer la garde d'un enfant à demander au juge qu'il ordonne l'inscription, sur le document d'identité, de la mention selon laquelle l'enfant ne peut franchir les frontières de l'espace Schengen sans son autorisation (voir Proposition de loi du 18 novembre 2010 modifiant le Code civil, la loi du 19 juillet 1991 (...) et modifiant la loi du 8 août 1983 (...) et l'arrêté royal du 10 décembre 1996 relatif aux pièces et certificats d'identité pour enfants de moins de douze ans, afin de prévenir l'enlèvement parental international d'enfants, Exposé des motifs, *Doc. parl.*, Chambre, 2013-2014, n° 0622/001, p. 8.) Cette loi n'est toutefois pas encore entrée en vigueur pour l'heure.

20. https://diplomatie.belgium.be/fr/Services/Protocole/Noblesse_et_ordres/noblesse/faq.

9 décembre 2019 modifiant l'arrêté royal du 25 mars 2003 a précisé que l'e-id comportait ce code-barres²¹. Un test effectué au moyen de l'insertion de notre carte d'identité dans un lecteur montre que ces données invisibles sont consultables par le citoyen lors d'une lecture numérique de la puce.

10. Le cas particulier des données biométriques (empreintes digitales) – Par une loi du 25 novembre 2018²², 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 »²³. La finalité poursuivie par l'enregistrement de cette information n'apparaît pas dans la loi, ce qui, comme on l'a dit précédemment, n'est pas conforme aux articles 8 C.E.D.H. et 22 de la Constitution.

Pour comprendre l'objectif poursuivi par le législateur, et comme exposé précédemment, 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'identité²⁴, en permettant aux services de police de vérifier l'exactitude du lien entre la carte d'identité et le porteur de celle-ci²⁵.

Dans l'avis négatif qu'elle a rendu au sujet de ce texte législatif, l'APD a déploré l'ajout de cette donnée, notamment en ce que « la prise d'empreintes digitales de la totalité d'une population n'est pas une mesure anodine sur le plan de la protection de la privée » et qu'il s'agit d'une mesure « intrusive par nature » devant être motivée et étayée pour répondre au respect du principe de proportionnalité²⁶. Or, selon l'APD, il n'est pas nécessaire d'ajouter les données biométriques, notamment en ce que « la carte d'identité comprend déjà un élément biométrique permettant de vérifier qu'elle appartient bien à son titulaire : la photo qui doit impérativement être changée à chaque changement de carte »²⁷. Et d'ajouter qu'en l'absence d'une « justification étayée et chiffrée sur des cas

avérés de fraudes liés à l'insuffisance des moyens de non falsification dont est dotée notre actuelle carte d'identité susceptible d'attester du caractère éventuellement insuffisant de la photo comme moyen d'authentification du porteur de la carte (...) la mesure apparaît disproportionnée »²⁸.

Par ailleurs, en février, mars et juin 2019, cinq recours en annulation contre l'article 27 de cette loi ont été introduits à la Cour constitutionnelle²⁹. Les requérants ont notamment soulevé que la disposition attaquée porte une atteinte injustifiée et disproportionnée au droit au respect de la vie privée dans la mesure où elle oblige les détenteurs d'une e-id à faire enregistrer leurs empreintes digitales sur celle-ci. Les requérants ont également pointé, tout comme l'avait fait l'APD, que cette disposition était dénuée de justification raisonnable quant à son objectif, les chiffres de fraude relayés dans les travaux préparatoires étant douteux et peu clairs³⁰. Ils en ont conclu à une violation du RGPD, en ce que le traitement des données relatives aux empreintes digitales va plus loin que ce qui est adéquat et nécessaire au regard de l'objectif poursuivi³¹.

Entre l'introduction des recours et le traitement de ceux-ci par la Cour, de nouvelles dispositions ont été adoptées au niveau européen. Un règlement européen du 20 juin 2019 « relatif au renforcement de la sécurité des cartes d'identité des citoyens de l'Union (...) »³² sera applicable dans l'Union européenne à partir du 2 août 2021. Il impose que les cartes d'identité nationales contiennent la photo de leur titulaire mais également « deux empreintes digitales dans des formats numériques interopérables »³³. L'objectif annoncé est de « renforcer la sécurité des cartes d'identité et des cartes de séjour »³⁴ en combinant « de manière appropriée une identification et une authentification fiables avec une réduction du risque de fraude »³⁵. Ce texte semble donc appuyer la volonté du législateur belge.

21. APD, avis n° 100/2019 du 3 avril 2019, *op. cit.*, n° 21.

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

23. Art. 27 de la loi du 25 novembre 2018 précitée.

24. 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.

25. *Ibid.*, p. 34.

26. APD, avis n° 19/2018 du 28 février 2018, n° 62 à 70. Dans le même sens, voir J. HERMANS et R. PEETERS, « Vingerafdrukken op de Belgische eID Technische analyse », accessible ici <https://www.esat.kuleuven.be/cosic/publications/article-3004.pdf>.

27. *Ibid.*, n° 67.

28. *Ibid.*, n° 69.

29. 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 Baudoïn 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 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.

30. C.C., arrêt n° 2/2021 du 14 janvier 2021 (n° de rôle 7125, 7150, 7202, 7203 et 7211), disponible à l'adresse : <https://www.const-court.be/public/f/2021/2021-002f.pdf>, points A.11 et A.18.3.1.

31. *Ibid.*, point A.23.3.

32. 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 »).

33. Art. 3.5 du Règlement 2019/1157.

34. Cons. 18 du Règlement 2019/1157.

35. *Idem.*

Néanmoins, la question de la proportionnalité demeurerait : est-il nécessaire d'enregistrer les empreintes digitales pour lutter contre la fraude à l'identité ? Le règlement UE n'apporte pas davantage de justification chiffrée que le législateur belge. Dans le cadre des recours introduits par les requérants contre la disposition attaquée, ceux-ci ont demandé à la Cour constitutionnelle de poser plusieurs questions préjudicielles à la Cour de justice de l'Union européenne, sur la validité du Règlement 2019/1157 au regard du droit au respect de la vie privée et du droit à la protection des données à caractère personnel. Ces dispositions consacrent le droit à la protection des données et exigent notamment que les données soient traitées loyalement, pour des finalités déterminées et sur la base d'un fondement légitime prévu par la loi.

La Cour constitutionnelle s'est prononcée tout récemment, par un arrêt du 14 janvier 2021, sur le bien-fondé de ces recours³⁶.

L'arrêt se déploie en trois temps puisque la Cour se prononce d'abord sur le prélèvement des empreintes et la conservation de l'image numérisée de celles-ci sur l'e-id³⁷, ensuite sur la conservation de l'image des empreintes pendant le temps de la fabrication et de la délivrance de la carte³⁸ et enfin sur la lecture de l'image de ces empreintes par les instances habilitées à cet effet³⁹.

A. Le prélèvement et la conservation de l'image numérisée des empreintes sur l'e-id

La Cour reconnaît que la disposition attaquée, en ce qu'elle prévoit le prélèvement de deux empreintes digitales et la conservation de l'image numérisée de celles-ci sur la carte d'identité, entraîne une ingérence dans le droit au respect de la vie privée et dans le droit à la protection des données⁴⁰. Ces empreintes étant des données sensibles au sens du RGPD, la Cour précise que ces données doivent être traitées en application du RGPD.

La Cour se penche ensuite sur les finalités poursuivies par la disposition attaquée, à savoir participer à la prévention des infractions liées à la fraude à l'identité, et indique que cette disposition poursuit le même objectif que celui poursuivi par le Règlement 2019/1157⁴¹. La Cour va même un pas plus loin, puisqu'elle affirme

qu'en réalité, la disposition attaquée vise à mettre en œuvre, anticipativement, la législation européenne⁴².

La Cour considère que ces objectifs sont légitimes, étant d'intérêt général et d'intérêt public important au sens du RGPD. Elle ajoute que la disposition attaquée est pertinente par rapport à ces objectifs et que le fait que le procédé ne permette pas d'exclure tout risque de fraude n'affaiblit pas cette proportionnalité⁴³. La Cour renvoie à ce propos à l'arrêt « *Schwartz c. Stadt Bochum* » de la Cour de justice, qui s'est prononcée dans le même sens s'agissant de l'insertion des empreintes digitales sur les passeports et de l'absence de fiabilité totale de ce procédé pour assurer la lutte contre la fraude.

La Cour examine ensuite le grief des requérants selon lequel la disposition attaquée viole le principe de légalité en ce qu'elle délègue son exécution au Roi, ce de manière insuffisamment précise puisque, notamment, le processus de fabrication et de délivrance des cartes d'identité n'est pas suffisamment décrit par la disposition légale⁴⁴. La Cour estime que la disposition attaquée est claire en ce qu'elle prévoit que les empreintes digitales sont disponibles uniquement sous forme numérisée lisible seulement électroniquement et que cette image numérisée est détruite au terme d'une période de trois mois maximum (période nécessaire à la fabrication et à la délivrance de l'e-id)⁴⁵. Celle-ci en déduit que le législateur a suffisamment précisé les éléments essentiels des mesures déléguées au Roi, de sorte que le principe de légalité prévu par l'article 22 de la Constitution est respecté⁴⁶.

Au terme de son analyse des griefs formulés par les requérants et les arguments du Conseil des ministres, la Cour en conclut que la disposition attaquée est proportionnée et nécessaire à la réalisation des objectifs poursuivis⁴⁷.

B. La conservation de l'image des empreintes pendant la fabrication et la délivrance de la carte

En ce qui concerne la conservation de l'image numérisée des empreintes digitales pour les besoins de la fabrication et de la délivrance de la carte, la Cour estime que dans la mesure où le délai de conservation est limité à 3 mois, que les travaux préparatoires de la loi indiquent que les données seront définitivement

36. C.C., arrêt n° 2/2021 du 14 janvier 2021 précité.

37. Points B.18 à B.36 de l'arrêt.

38. Points B.37 à B.39 de l'arrêt.

39. Points B.40 à B.44 de l'arrêt.

40. C.C., arrêt n° 2/2021 du 14 janvier 2021 précité, point B.19.1.

41. *Ibid.*, point B.19.2., p. 52.

42. *Ibid.*, point B.20.1., p. 54.

43. *Ibid.*, point B.20.2.

44. *Ibid.*, point B.18, p. 50.

45. *Ibid.*, point B.23.1.

46. *Ibid.*, point B.23.2.

47. *Ibid.*, points B.29 et B.31.2.

supprimées ensuite, et que le Roi doit prendre des mesures pour garantir l'intégralité et la confidentialité des données, le droit au respect de la vie privée et à la protection des données à caractère personnel des citoyens est respecté⁴⁸.

C. La lecture de l'image des empreintes digitales par les instances habilitées à cet effet

La Cour en arrive à la même conclusion s'agissant de la lecture ultérieure de l'e-id et des empreintes digitales y contenues. Elle considère que seules les personnes habilitées listées dans la loi peuvent lire l'e-id, et que cette lecture n'implique pas un enregistrement des données (ce qui empêcherait le croisement de données aux fins d'identifier un individu)⁴⁹. La Cour rappelle qu'il appartient également au Roi de prendre des mesures techniques adéquates pour déterminer les modalités concrètes de lecture de ces empreintes. Elle indique également que seul le personnel chargé du contrôle aux frontières, en Belgique et à l'étranger, doit pouvoir lire ce type de données, et uniquement dans le cadre de la lutte du contrôle aux frontières⁵⁰. Les habilitations des services de police sont également, selon la Cour, suffisamment encadrées.

Sur la base de ces constats, la Cour rejette les recours. Elle refuse, dans le même temps, de poser quelque question préjudicielle à la Cour de justice.

Ainsi, la Cour semble faire fi de toute préoccupation liée au principe de légalité que nous avons exposé précédemment. Bien que la loi soit très succincte et peu claire sur les modalités entourant le prélèvement des empreintes digitales, leur numérisation, leur conservation et leur lecture, cela semble suffisant pour la Cour constitutionnelle, qui semble avoir toute confiance en l'exécutif et qui se retranche, au fil de sa motivation, derrière le règlement européen adopté en la matière. Le citoyen devra donc faire preuve d'une certaine confiance envers ceux qui prélèveront, et liront leur e-id et les empreintes digitales qu'elle contient.

IV. Quelles utilisations peut-on faire l'e-id ?

11. Quelle autorité ou personne/quelle donnée/quel traitement – Ainsi qu'on l'a dit précédemment⁵¹,

l'e-id peut être demandée à un citoyen dans le but de l'identifier.

Si, dans un cas d'espèce, la visualisation, à l'œil nu, de la carte suffit pour identifier la personne au départ des données inscrites sur cette carte, c'est la solution qui doit être privilégiée, car elle ne constitue pas un traitement de données.

Par exemple, si un vendeur de boissons alcoolisées a des doutes sur l'âge d'un client souhaitant acheter une bouteille d'alcool, il lui suffit de regarder, sur la carte, sa date de naissance et, éventuellement, sa photo en cas de suspicion de fraude⁵².

S'il est nécessaire d'identifier plus précisément la personne, pour lire électroniquement certaines données ou pour les enregistrer, la légalité de cette demande d'identification dépend de la qualité de la personne qui demande d'utiliser l'e-id d'un citoyen (s'agit-il d'un acteur du secteur public ou du secteur privé ?), du type de données utilisées (s'agit-il d'une donnée dont l'utilisation est soumise à une autorisation spécifique ?) et du type d'usage envisagé.

A. L'autorité ou la personne qui utilise l'e-id d'un citoyen

12. Base légale – Que la personne qui demande d'utiliser l'e-id émane du secteur public ou du secteur privé, elle doit pouvoir fonder cette demande sur une base légale. Celle-ci varie selon le secteur concerné.

13. Secteur public – L'article 6, § 7, de la loi du 19 juillet 1991 habilite le Roi à déterminer « les autorités et officiers publics sur la réquisition desquels la carte doit être présentée ».

Il est regrettable que le législateur ne précise pas davantage cette habilitation. En effet, le pouvoir du Roi d'exécuter les lois, visé à l'article 108 de la Constitution, suppose que la loi soit suffisamment précise pour que la compétence du Roi ne porte que sur « l'exécution de mesures dont les éléments essentiels sont fixés par le législateur »⁵³ et que le Roi « n'étende pas la portée de la loi, ni ne la restreigne »⁵⁴.

Or, en l'espèce, les termes « autorités et officiers publics » ne sont pas suffisamment précis pour confier

48. *Ibid.*, point B.37 et 38.1.

49. *Ibid.*, point B.41.3.

50. *Ibid.*, point B.42.1.

51. Cf. n° 2 et n° 7.

52. Cet exemple est fourni par l'APD <https://www.autoriteprotectiondonnees.be/professionnel/themes/eid/lecture>.

53. C.C., arrêt n° 95/2008, B.42 ; arrêt n° 29/2010, B.16. En ce sens également, avis L. 37.765/1/2/3/4 du 4 novembre 2004 sur un avant-projet de loi-programme, *Doc. parl.*, Chambre, 2004-2005, n° 1437 ; avis L. 37.748 et 37.749/AG du 23 novembre 2004 sur un avant-projet de loi modifiant la loi du 11 décembre 1998 relative à la classification et aux habilitations de sécurité (37.748/AG) et sur un avant-projet de loi modifiant la loi du 11 décembre 1998 portant création d'un organe de recours en matière d'habilitation de sécurité (37.749/AG), *Doc. parl.*, Chambre, 2004-2005, n° 1598/1 et 1599/1.

54. Cass., 18 novembre 1924, *Pas.*, 1925, I, p. 25 ; Cass., 19 janvier 1959, *Pas.*, I, p. 494 ; Cass., 15 mars 1965, *Pas.*, I, p. 740 ; Cass., 5 mai 1970, *Pas.*, I, p. 766. Avis L. 39.514/1 relatif à un projet d'arrêté royal portant création et fixant la composition et les modalités de fonctionnement du Comité chargé de la qualité des données de la Banque-Carrefour des Entreprises et de son fonctionnement, du 29 novembre 2005, *M.B.*, 28 février 2006 ; avis L. 38.235/2 du 11 avril 2005 relatif à un projet d'arrêté royal déterminant les types d'informations associées aux informations visées à l'article 3, alinéa 1^{er}, de la loi du 8 août 1983 organisant un registre national des personnes physiques, *M.B.*, 25 janvier 2006 ; R. ANDERSEN et P. NIHOUL, « Le Conseil d'Etat. Chronique de jurisprudence 1998 », *R.B.D.C.*, 2000/1, pp. 91 et 92. Pour plus d'informations à ce sujet, voir E. DEGRAVE, *Le-gouvernement et la protection de la vie privée (...)*, *op. cit.*, n° 109 et s.

au Roi la seule exécution des mesures législatives. En effet, des questions importantes, qui définissent la portée de la loi, restent en suspens. Par exemple, est-ce la seule qualité d'autorité publique ou d'officier public qui permette la réquisition de la carte ou cette réquisition est-elle conditionnée au respect de certaines finalités ? Une fois la carte réquisitionnée, que peut-il en être fait ? Ce sont des éléments essentiels dont la réponse devrait être fixée par le législateur.

A la place de cela, la portée réelle de la loi est, *de facto*, définie dans l'article 1^{er} de l'arrêté royal du 25 mars 2003.

Celui-ci précise l'habilitation législative au regard à la fois du type d'autorité publique qui réquisitionne la carte, du type de démarche administrative entamée par le citoyen et du type de finalité poursuivie.

Ainsi, la police et l'huissier de justice chargé de la signification d'un exploit peuvent réquisitionner la carte d'identité, de par leur qualité.

Les autres autorités et officiers publics peuvent réquisitionner la carte dans les cas suivants : lorsque le citoyen fait une déclaration, ou demande un certificat. Les termes « déclaration » et « certificats » ne sont pas définis dans l'arrêté royal.

Ils peuvent également réquisitionner la carte « de manière générale, lorsqu'il s'agit d'établir l'identité du porteur »⁵⁵.

Ainsi qu'on le voit, le flou entourant l'habilitation législative a pour conséquence que le Roi est amené à définir lui-même des éléments essentiels de la loi, et à outrepasser les compétences qui sont les siennes en vertu de l'article 108 de la Constitution.

14. Secteur privé – Les acteurs du secteur privé ne peuvent quant à eux lire ou utiliser l'e-id d'un client que si ce dernier y a consenti, de manière libre, spécifique et éclairée ou bien s'ils y sont obligés en vertu d'une disposition légale⁵⁶. Il s'agit d'une transposition dans la loi belge de deux bases légales prévues par le RGPD et permettant de rendre licite un traitement de données⁵⁷.

La première hypothèse se rencontre par exemple dans le cas des commerces qui souhaitent utiliser la carte d'identité de leurs clients comme carte de fidélité, pour éviter de devoir remplir un formulaire papier ou de créer une carte distincte. Dans ce cas, ces

commerces doivent bien veiller à obtenir le consentement parfaitement libre et éclairé de leurs clients avant d'utiliser leur carte, ce qui implique de les informer sur la manière dont les données qui y sont contenues vont être utilisées, et pour quelles raisons. La loi du 19 juillet 1991⁵⁸ prévoit par ailleurs que si la lecture de la carte se fait au moyen d'une application informatique, le citoyen doit pouvoir se voir offrir une alternative à la lecture de son document d'identité pour bénéficier du programme de fidélité. En d'autres termes, le citoyen ne doit pas se sentir obligé d'accepter que le commerçant utilise son e-id pour pouvoir bénéficier du programme de fidélité. Cela implique également ne pas influencer fortement le choix du client en lui proposant, par exemple, un bon de réduction s'il accepte d'utiliser son e-id, bon de réduction qui ne serait pas proposé en cas de création d'une carte de fidélité classique. Dans un tel cas, on ne pourrait pas considérer que le consentement du client au traitement de son e-id serait « libre ».

L'APD a récemment infligé une amende à un commerçant qui utilisait la carte d'identité de ses clients comme carte de fidélité, en ne leur offrant aucune autre alternative⁵⁹. La chambre contentieuse a estimé, sur la base de l'article 6, § 4, al. 3, de la loi du 19 juillet 1991 ainsi que du RGPD que trois infractions devaient être constatées dans le chef du commerçant : une violation du principe de minimisation des données (car les données collectées comprenaient le numéro de registre national – repris dans le code-barres de la carte d'identité –, le sexe et la date de naissance du client, données qui ne sont pas pertinentes pour l'utilisation recherchée) (i), une atteinte au principe de légalité du traitement (faute d'un consentement libre dans le chef du citoyen qui n'avait d'autre choix que de présenter sa carte d'identité pour bénéficier du programme de fidélité) (ii) et une violation du principe de transparence (la politique de confidentialité du commerçant ne reprenant pas les exigences imposées par le RGPD) (iii).

La décision a fait l'objet d'un recours devant la Cour des marchés, qui l'a invalidée⁶⁰. La Cour a en effet constaté que l'APD s'est basée sur l'article 6, § 4, al. 3 dont question, alors qu'il n'était pas encore applicable au moment du dépôt de la plainte, de sorte que le commerçant n'était à l'époque pas tenu d'offrir une alternative au citoyen ni d'obtenir son consentement libre, spécifique et éclairé. S'agissant du consentement, la Cour a estimé que la chambre contentieuse avait erronément considéré qu'en ne pouvant bénéficier de réductions que par le biais de la carte de fidélité et donc

55. Voir également les explications pratiques fournies par l'APD <https://www.autoriteprotectiondonnees.be/professionnel/themes/eid/presentation>.

56. Loi du 19 juillet 1991, *op. cit.*, art. 6, § 4, al. 2.

57. RGPD, art. 6.1., a) et c).

58. Loi du 19 juillet 1991, *op. cit.*, art. 6, § 4, al. 3.

59. Autorité de protection des données (chambre contentieuse), décision 06/2019 du 17 septembre 2019, disponible sur : <https://www.autoriteprotectiondonnees.be/citoyen/publications/decisions>, onglet « Décision de la Chambre Contentieuse ».

60. Bruxelles (sect. Cour des marchés, 19^e ch. A), 19 février 2020 (R.G. n° 2019/AR/1600), disponible sur : <https://www.autoriteprotectiondonnees.be/citoyen/publications/decisions>.

la présentation de sa carte d'identité, sans alternative, le consentement du client n'était pas libre. Selon la Cour, le client, en ne présentant pas sa carte d'identité, ne subit pas d'inconvénient mais perd seulement la possibilité de bénéficier d'un avantage. En ce sens, son consentement n'est donc pas forcé. La Cour a annulé la décision de l'APD, condamnée à rembourser l'amende payée par le commerçant.

La Cour des marchés, si elle se penchait certes sur une décision de l'APD prise en exécution d'un alinéa de la loi qui n'était pas en vigueur au moment des faits, est regrettable sur le plan de la protection des données à caractère personnel du citoyen. En effet, en obligeant le citoyen à présenter sa carte d'identité sans lui proposer d'autre possibilité, le commerçant oriente bel et bien le choix du client qui souhaite bénéficier de l'avantage du programme de fidélité.

La deuxième hypothèse dans laquelle un acteur du secteur privé peut solliciter la lecture de la carte d'identité est celle d'une obligation légale. On peut citer, au titre d'exemple, la loi anti-blanchiment⁶¹ qui oblige divers professionnels (banques, institutions de crédit, assureurs, avocats, ...) à prendre une copie, sur support papier ou électronique, de la carte d'identité de leurs nouveaux clients. Le but est d'empêcher l'ouverture de comptes ou les transferts de sommes d'argent importantes sous de faux noms ou des pseudonymes pour faciliter le blanchiment d'argent. La loi du 1^{er} septembre 2016 a également imposé aux opérateurs téléphoniques (par l'intermédiaire, souvent, des magasins de téléphonie) d'identifier les clients qui entendent se procurer une carte prépayée, ce afin de participer à la lutte contre le terrorisme⁶².

B. Le type de données traitées

15. Données générales et données spécifiques – Que l'autorité ou la personne prétendant utiliser l'e-id d'un citoyen émane du secteur public ou du secteur privé, certaines données sont protégées par le régime général du RGPD. On les qualifie de « données générales ». D'autres données sont spécifiquement protégées par une législation particulière. On les qualifie de « données spécifiques ».

a) Données générales

16. Principe de minimisation des données – Le principe de minimisation des données, consacré par l'article 5.1., c), du RGPD, doit être respecté à chaque

utilisation de l'e-id. Cela signifie que seules les données nécessaires à l'objectif poursuivi peuvent être traitées.

Pour illustrer cette exigence, reprenons les exemples très pertinents fournis par l'APD sur son site internet. Si un commerçant vend de l'alcool via un distributeur automatique requérant la lecture de la e-id, le vendeur doit s'assurer que seule la date de naissance sera lue⁶³. Autre exemple, si une piscine communale offre un tarif préférentiel aux habitants de la commune, il faut s'assurer que seul le code postal sera lu⁶⁴.

A cet égard, l'utilisation de la carte d'identité comme carte de fidélité pose également question. En effet, si l'objectif est uniquement de proposer un programme de fidélité, une carte de fidélité « unique » et des réductions à un client, seule la lecture de certaines données comme les noms et prénoms, voire l'adresse postale et dans certaines circonstances la date de naissance (pour proposer une action « anniversaire » par exemple) semble pouvoir avoir lieu. On voit en effet mal comment un commerçant pourrait justifier avoir besoin du lieu de naissance du client, de son numéro de registre national ou encore du numéro de sa carte d'identité et des certificats y afférents. Dans les faits toutefois, il est loin d'être certain que les commerçants ne profitent pas de la lecture de la carte d'identité pour récolter plus de données que nécessaire et les utiliser à des fins de marketing direct, voire pour les commercialiser.

Déjà en 2012, la société Fidel ID a été condamnée judiciairement parce qu'elle commercialisait un système de fidélité (« Freedility ») basé sur l'utilisation de la carte d'identité des consommateurs pour des fins strictement commerciales (fidélisation, statistiques, suivi de clientèle, etc.). Ce système collectait notamment le numéro de Registre national des citoyens, dont on verra ci-après qu'il constitue en plus une donnée spécifiquement protégée. La Cour d'appel de Bruxelles a condamné cette pratique et ordonné à la société Fidel ID de cesser d'utiliser ce numéro de Registre national, considérant ce procédé comme illégal⁶⁵.

Ce type de système de fidélité existe pourtant toujours et se déploie⁶⁶. A la lecture du site internet de Freedility, on comprend que ce système permet à ses initiateurs de tracer les achats réalisés par les clients dans les commerces utilisant le système de fidélité et

61. Loi du 18 septembre 2017 relative à la prévention du blanchiment de capitaux et du financement du terrorisme et à la limitation de l'utilisation des espèces, *M.B.*, 6 octobre 2017.

62. Loi du 1^{er} septembre 2016 portant modification de l'article 127 de la loi du 13 juin 2005 relative aux communications électroniques et de l'article 16/2 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité, *M.B.*, 7 décembre 2016.

63. <https://www.autoriteprotectiondonnees.be/professionnel/themes/eid/lecture>.

64. <https://www.autoriteprotectiondonnees.be/professionnel/themes/eid/applications-pratiques>.

65. Pour plus d'informations à ce sujet voir : Bruxelles, 9 mai 2012, *J.T.* 2012, n° 33, p. 690 et note d'observations E. DEGRAVE, « La carte d'identité électronique utilisée comme carte de fidélité : un traitement de données à caractère personnel illégal sanctionné par la cour d'appel de Bruxelles », *J.T.* 2012, n° 33, 691-693 ; J.-M. VAN GYSEGHEM, « La carte d'identité électronique et les apprentis sorciers », *R.D.T.I.*, 2014/2, 87-94.

66. La liste des commerces participants au programme de fidélité « Freedility » est disponible à l'adresse : <https://www.freedility.be/repertoire-des-commerces>.

de croiser ces informations aux données figurant sur la puce de leur carte d'identité. Ceci permet d'établir un profil consommateur, accessible aux commerces utilisant le système Freedelity, pourvu que le client ait accepté que son profil soit partagé⁶⁷. La tentation de s'écarter de la finalité pour laquelle l'e-id est lue, à savoir proposer une carte de fidélité « unique » à ses clients et éviter de remplir des formulaires papier, semble donc bien présente. Elle se couple bien souvent avec un défaut d'information du client, qui n'a aucun moyen de savoir ce qu'on fait de sa carte d'identité une fois qu'elle passe de l'autre côté du comptoir.

b) Données spécifiques

17. Législation spécifique – Certaines données sont protégées par une législation spécifique, qui inclut cette exigence de minimisation des données mais impose des restrictions supplémentaires. C'est le cas du Numéro d'identification au Registre national, de la photo et des empreintes digitales⁶⁸.

18. Numéro de Registre national (NIRN) – Le NIRN est un identifiant propre à chaque citoyen, composé de sa date de naissance dans le format année/mois/jour, d'un chiffre correspond au compteur journalier des naissances et d'un chiffre de contrôle. L'usage de cet identifiant a été généralisé au sein de l'administration si bien que le NIRN est également le numéro fiscal⁶⁹, le numéro de sécurité sociale⁷⁰, le numéro de santé de chaque personne⁷¹ et le numéro généralement utilisé pour les échanges de données au sein de l'administration. On peut donc le qualifier d'identifiant universel. Cela explique que ce numéro doit être manié avec prudence, puisqu'il permet de retrouver chaque citoyen dans toutes les bases de données de l'Etat.

Pour cette raison, le NIRN ne peut être utilisé que « par ou en vertu d'une loi, d'un décret ou d'une ordonnance »⁷². C'est l'article 8 de la loi du 8 août 1983⁷³ qui définit les conditions à remplir pour pouvoir utiliser ce numéro. En somme, l'utilisation du NIRN est réservée à certaines autorités, qui poursuivent des missions d'intérêt général légalement encadrées⁷⁴.

Ces autorités doivent obtenir l'autorisation du ministre de l'Intérieur, qui est chargé de vérifier, notamment et dans chaque cas d'espèce, si l'usage du NIRN est nécessaire⁷⁵.

19. La photographie – La photographie du titulaire de l'e-id est placée sur l'e-id dans le but de comparer la personne physique à sa photo, en cas de suspicion de fraude. On peut ainsi s'assurer que cette personne est bien le bon titulaire de l'e-id.

La photographie n'est pas une donnée anodine. Elle présente un risque particulier en termes de fraude puisqu'elle peut faciliter la création de fausses cartes d'identité⁷⁶.

C'est pourquoi, tout comme le NIRN, la photographie ne peut être utilisée que « par ou en vertu d'une loi, d'un décret ou d'une ordonnance »⁷⁷. C'est l'article 6*bis*, de la loi du 19 juillet 1991 qui détermine les conditions d'utilisation de la photo. Ainsi, la photo ne peut être utilisée que par certaines autorités⁷⁸ – celles-là mêmes qui peuvent utiliser le NIRN – à la condition d'avoir obtenu l'autorisation du ministre de l'Intérieur⁷⁹.

20. L'image numérisée des empreintes digitales – Compte tenu de son caractère sensible, le traitement de l'image numérisée des empreintes digitales dont il a été question plus haut est réservé à certaines autorités publiques limitativement énoncées à l'article 6, § 2, de la loi du 19 juillet 1991. Il s'agit notamment du personnel des communes chargé de la délivrance des cartes d'identité, des services de police, des membres du personnel de l'Office des étrangers, etc. Dans le cadre de leur recours devant la Cour constitutionnelle, les requérants ont soulevé, notamment, que l'habilitation donnée aux autorités pour lire ces données figurant sur l'e-id était trop large. Ils ont pris l'exemple d'agents chargés du contrôle des frontières à l'étranger, qui pourraient travailler pour une firme privée⁸⁰. La Cour a jugé que les autorités chargées du contrôle aux frontières devaient toujours être autorisées par les autorités nationales compétentes ou par des agences de l'Union, ainsi que le prévoit le Règlement 2019/1157⁸¹.

67. <https://www.freedelity.be/questions-et-reponses> (« Mes données personnelles sont-elles transmises à des tiers ? »).

68. Ces données sont explicitement reprises à l'article 6, § 4, de la loi du 19 juillet 1991.

69. Art. 314, § 1, C.I.R. 92.

70. Art. 7 et 8 de la loi du 15 janvier 1990 sur la Banque-Carrefour de la sécurité sociale.

71. Pour plus d'informations, voir [https://ehealth.fgov.be/fr/esante/professionnels-de-la-sante/ehealthcreabis/presentation-generale#:~:text=Le %20m %C3 %A9decin %20doit %20transmettre %20le,de %20contact %20est %20 %C3 %A9galement %20disponible](https://ehealth.fgov.be/fr/esante/professionnels-de-la-sante/ehealthcreabis/presentation-generale#:~:text=Le%20m%C3%A9decin%20doit%20transmettre%20le,de%20contact%20est%20%C3%A9galement%20disponible).

72. Art. 6, § 4, de la loi du 19 juillet 1991.

73. Loi du 8 août 1983 organisant un registre national des personnes physiques.

74. Ces autorités sont énoncées à l'article 5, § 1, de la loi du 8 août 1983.

75. Pour plus d'informations, voir l'article 8 de la loi du 8 août 1983 précitée ainsi que les explications fournies par l'APD sur son site internet <https://www.autoriteprotectiondonnees.be/professionnel/themes/eid/lecture>.

76. En ce sens, <https://www.autoriteprotectiondonnees.be/professionnel/themes/eid/lecture>.

77. Art. 6, § 4, de la loi du 19 juillet 1991.

78. Il s'agit des autorités visées à l'article 5, 61, de la loi du 8 août 1983.

79. Art. 6*bis*, § 3, de la loi du 19 juillet 1991. Pour plus d'informations pratiques, voir <https://www.autoriteprotectiondonnees.be/professionnel/themes/eid/lecture>.

80. C.C., arrêt n° 2/2021 du 14 janvier 2021 précité, point B.42.1.

81. C.C., arrêt n° 2/2021 du 14 janvier 2021 précité, point B.42.2.2.

C. Le type de traitement effectué

a) Un traitement nécessaire

21. Proportionnalité – Outre le fait que la demande de traiter l'e-id doit être fondée sur une base légale qui varie en fonction du secteur public ou privé, et qu'il faille traiter un minimum de données, l'usage concret de l'e-id doit également être limité au strict nécessaire. Il s'agit de l'exigence de proportionnalité du traitement de données⁸².

Ainsi qu'on l'a dit d'emblée, si la lecture à l'œil nu de la carte d'identité suffit pour identifier la personne, il n'y a pas lieu de passer cette carte dans un lecteur d'e-id.

Dans les cas où il est nécessaire de lire électroniquement la carte, il n'est pas pour autant nécessaire d'enregistrer les données lues.

Pour reprendre l'exemple de la vente d'alcool évoqué précédemment, si la vente d'alcool se fait via un distributeur automatique, il sera nécessaire de lire la date de naissance sur la carte d'identité. Pour autant, il n'est en principe pas nécessaire que le commerçant enregistre l'identité du client. Dans le même sens, une piscine communale qui offre un tarif préférentiel aux habitants de la commune a besoin de lire le code postal mais il n'est pas nécessaire d'enregistrer dans sa base de données l'identité de la personne ayant accédé à la piscine.

b) Le citoyen peut-il contrôler l'utilisation de son e-id ?

22. « Privacy by design » – Au moment où le citoyen confie son e-id à un tiers, comment peut-il savoir si les données de sa carte seront lues ou enregistrées et lesquelles de ses données seront lues et/ou enregistrées ?

Juridiquement, les personnes et les autorités qui utilisent l'e-id sont obligées d'informer le citoyen du traitement qui est fait de cette donnée, en vertu de l'article 13 du RGPD. Par exemple, une autorité qui procède à la lecture des empreintes digitales doit en informer la personne, en expliquant la raison d'être de cette consultation et ses modalités.

Néanmoins, en pratique, il pourrait arriver que la personne ou l'autorité utilisant l'e-id d'un citoyen ne respecte pas les exigences légales, en n'informant pas ce citoyen ou en violant les limites imposées par la loi⁸³. A cet égard, l'APD est très franche quand, à propos

de la loi du 19 juillet 1991 qui limite l'utilisation de la photo, elle affirme qu'il s'agit d'« un beau principe qui ne vaut rien dans la pratique. La photographie, qui est aussi obligatoirement enregistrée sur la puce de manière numérisée, n'est protégée en aucune manière. L'autorité publique fournit donc au citoyen un instrument n'offrant pas une protection spécifique pour cette donnée. Le citoyen n'a aucun contrôle des données qui peuvent ou non être lues de manière électronique »⁸⁴. Et de poursuivre ainsi : « le citoyen se trouve démuné. Il est tout simplement obligé de se baser sur la bonne foi de chaque personne qui lit sa carte d'identité. Lorsqu'il consent à la lecture de sa carte, il n'a aucune garantie que les informations qui sont lues, dont la photographie, ne sont pas non plus enregistrées. Lorsque sa carte est volée ou qu'il la perd, le vol d'identité est toutefois très facile »⁸⁵.

A l'heure actuelle, ce constat surprend. En effet, depuis le 25 mai 2018 et l'entrée en application du RGPD, le principe de protection des données dès la conception (dit aussi « *privacy by design* ») doit être respecté. Il s'agit, pour chaque responsable d'un traitement de données – comme l'Etat pour l'e-id – de veiller à mettre en place les mesures techniques et organisationnelles qui permettent de garantir la protection de la vie privée dès la conception de l'outil, en veillant, par exemple, à ce que, techniquement, on ne puisse pas traiter plus de données que nécessaires. En d'autres termes, la régulation technique doit soutenir le respect effectif de la régulation juridique.

En l'espèce, ce principe conduit à considérer que des mesures concrètes doivent être prises, qui permettent au citoyen de visualiser, au moment où sa carte est intégrée dans un lecteur, quelles sont ses données qui sont lues et/ou enregistrées. Dans certains cas, il devrait également pouvoir choisir lui-même les données qu'il choisit de communiquer, et l'usage qui peut en être fait (lecture, enregistrement, réutilisation ultérieure).

De telles mesures pourraient être mises en place, par exemple, via des lecteurs d'e-id plus perfectionnés que les lecteurs actuels.

Par exemple, lorsqu'il n'est pas nécessaire, pour le tiers qui réclame la e-id, d'accéder à l'identité parfaite du citoyen, ce dernier devrait pouvoir visualiser les données qui sont traitées, en vertu de son droit à l'information, consacré à l'article 13 RGPD.

En outre, lorsque seules certaines données doivent nécessairement être communiquées – comme dans l'exemple précité d'une piscine communale qui doit

82. Le principe de proportionnalité du traitement est concrétisé par l'article 6, b) à f), du RGPD qui exige que le traitement soit « nécessaire » pour atteindre les objectifs mentionnés.

83. C'est d'ailleurs ce qu'avait fait la société Fidel ID à propos de l'utilisation du NIRN (cf. *supra*, n° 15).

84. APD, avis n° 100/2019 précité, n° 17.

85. APD, avis n° 100/2019 précité, n° 19.

vérifier le code postal de la personne pour lui octroyer un tarif préférentiel – il y aurait lieu de recourir à un lecteur de carte qui, dans sa conception technique, limite la lecture de la carte au seul code postal et permette au citoyen de visualiser le fait que seule cette donnée est lue par le lecteur.

Par ailleurs, lorsque le fait de confier son e-id est fondé sur le consentement libre, spécifique et éclairé⁸⁶, il y aurait lieu de permettre au citoyen de sélectionner les données qu'il communique dans le but de créer une carte de fidélité. Il lui reviendrait de choisir s'il communique son adresse postale ou uniquement un mail, de décider s'il donne sa date de naissance etc. et ce, en vertu de son droit de consentir de manière libre et éclairée au traitement de ses données. En guise d'illustration, le fait, pour un commerçant, de proposer une carte de fidélité au départ de l'e-id, ne devrait être autorisé légalement qu'à la condition que ce commerçant utilise un lecteur e-id qui, en lui-même, permette au citoyen de choisir les données qu'il accepte de communiquer au commerçant. Ainsi, le citoyen devrait pouvoir décider qu'il communique son adresse postale comme point de contact pour le commerçant, mais non sa date de naissance.

En 2018, l'APD a recommandé au législateur « d'imposer aux responsables de traitement concernés de mettre en place des outils permettant à la personne concernée de décider des données qu'elle communique au moyen de sa carte »⁸⁷. Malheureusement, le législateur n'a pas suivi cette recommandation, arguant du fait que « cette possibilité n'est pas envisageable car trop complexe pour le citoyen »⁸⁸. Cette affirmation n'a pas convaincu l'APD qui, à juste titre selon nous, rappelle que « le concept de carte d'identité électronique date d'il y a 15 ans » et se pose la question de savoir si « entre-temps, on a examiné sérieusement la question de savoir si compte tenu de l'état actuel de la technologie, il est possible de délivrer au citoyen une carte lui permettant de mieux protéger ses données », concluant qu'« actuellement, la carte d'identité peut difficilement être considérée comme un exemple de *privacy by design* (protection de la vie privée dès la conception) »⁸⁹.

c) Une certaine transparence en ligne pour les données traitées par l'administration

23. « Mon dossier » au Registre national – Signalons une utilisation intéressante de l'e-id pour tout citoyen

curieux d'en savoir plus sur le traitement de ses données par l'administration Il s'agit de l'outil « Mon dossier » du registre national⁹⁰.

Cet outil a été créé il y a plus de dix ans par le SPF Intérieur, qui gère le Registre national. Après s'être identifié avec son e-id, chaque citoyen peut accéder à un portail qui lui permet de voir l'ensemble de ses données enregistrées au Registre national. Un onglet lui permet de signaler les erreurs affectant ses données, le cas échéant.

Le citoyen peut aussi cliquer sur l'onglet « Qui consulte mes données », et voir apparaître le nom des institutions s'étant intéressées à lui dans les six derniers mois⁹¹. Il peut ainsi, le cas échéant, demander à l'institution mentionnée les raisons de telles consultations et en vérifier la légalité.

Conclusion

La carte d'identité est l'outil clé de la vie administrative du citoyen, depuis plus de 100 ans. Dans sa version électronique, elle existe depuis plus de 15 ans.

Pourtant, la présente étude a montré que l'encadrement normatif est embroussaillé et peu clair. S'agissant particulièrement des exigences européennes et constitutionnelles liées à l'utilisation des données à caractère personnel figurant sur cette carte, la matière souffre de nombreuses lacunes législatives. Actuellement, les règles sont disséminées entre plusieurs lois et plusieurs arrêtés royaux, dont la compréhension passe bien souvent par la lecture des travaux préparatoires de ces textes. On y décèle également des anachronismes étonnants⁹². Par ailleurs, peu de réflexions semblent avoir été menées sur la manière dont la technique pourrait assurer l'effectivité des règles de droit, via des lecteurs e-id plus performants, par exemple.

Or, ainsi qu'on l'a montré, l'usage de l'e-id s'étend. Il n'est plus limité aux démarches administratives du citoyen. Il intervient désormais dans le secteur privé, soucieux d'identifier correctement chaque personne. Les données enregistrées sur cette carte sont également de plus en plus nombreuses et sensibles, comme en témoigne la récente intégration de l'image numérisée des empreintes digitales.

86. Art. 6.1., a), RGPD.

87. APD, avis n° 19/2018 précité, n° 75.

88. Chambre, Projet de loi portant des dispositions diverses concernant le Registre national et les registres de population, *Doc. parl.*, sess. 2017-2018, 54 3256/001, p. 39.

89. APD, avis n° 100/2019, n° 18.

90. Lien vers l'outil : <http://www.ibz.rn.fgov.be/fr/registre-national/mon-dossier/>.

91. Cette possibilité est organisée par l'article 6, § 3, 3°, de la loi du 19 juillet 1991 qui ne permet toutefois pas l'accès aux informations concernant les traitements de données effectués par « les autorités administratives et judiciaires chargées de la recherche et de la répression des délits ainsi que de la Sûreté de l'Etat et du Service général du renseignement et de la sécurité des Forces armées ».

92. Par exemple, l'article 6, § 9, de la loi du 19 juillet 1991 autorise le Roi à étendre l'application de la loi moyennant l'autorisation du comité sectoriel du registre national... qui n'existe plus depuis 2018.

Le citoyen n'a pas le choix : il est contraint de disposer d'une e-id personnelle, contraint d'accepter qu'y soient placées des données nombreuses et parfois délicates, contraint de l'utiliser dans sa relation avec l'Etat, et de plus en plus souvent encouragé à le faire dans ses liens avec le secteur privé. Or, l'e-id souffre d'un manque évident de transparence et de pédagogie par rapport au citoyen, tant dans son contenu que dans son usage. C'est un constat qui ne peut perdurer, au risque, progressivement, d'ébranler la confiance de chacun dans les outils numériques, de plus en plus nombreux, qui sont mis en place par l'Etat pour gérer les politiques publiques.

Partant de ces constats, il serait judicieux, au regard notamment de l'exigence de légalité qui fonde toute ingérence dans la vie privée des citoyens, que le législateur remette l'ouvrage sur le métier. Il est devenu nécessaire que la Belgique se dote d'une loi, claire, précise et prévisible, dédiée exclusivement à la carte d'identité électronique. Une loi qui fixe notamment

la liste limitative des données qui peuvent y être enregistrées et, pour chacune de ces données, les finalités pour lesquelles elles peuvent être traitées. Cette loi devrait également imposer des exigences claires en termes de régulation technique, en conditionnant par exemple l'usage de l'e-id par certains acteurs, à l'obligation de disposer d'un lecteur de carte qui, en lui-même, empêche l'accès aux données non nécessaires, tout en permettant à chacun de visualiser sur un écran les données qui sont lues et/ou enregistrées par un tiers. Enfin, cette loi devrait également clarifier le contrôle des acteurs qui utilisent l'e-id et prévoir des sanctions claires et adéquates pour tout qui ne respectent pas les exigences encadrant cet outil.

C'est là une belle occasion de définir, dans l'ère numérique, l'équilibre entre l'efficacité administrative et la vie privée de chacun, pour nourrir la nécessaire confiance entre le citoyen et ses différents partenaires, publics et privés.