

Version anonymisée

Traduction

C-61/22 - 1

Affaire C-61/22

Demande de décision préjudicielle

Date de dépôt :

1^{er} février 2022

Juridiction de renvoi :

Verwaltungsgericht Wiesbaden (Allemagne)

Date de la décision de renvoi :

13 janvier 2022

Partie requérante :

RL

Partie défenderesse :

Landeshauptstadt Wiesbaden

[OMISSIS]

VERWALTUNGSGERICHT WIESBADEN
(TRIBUNAL ADMINISTRATIF DE WIESBADEN, ALLEMAGNE)

ORDONNANCE

Dans la procédure administrative contentieuse

RL

[OMISSIS],

Partie requérante

[OMISSIS]

contre

FR

Landeshauptstadt Wiesbaden (Wiesbaden, capitale du Land de Hesse)
[OMISSIS] Wiesbaden,

Partie défenderesse

ayant pour objet : Réglementation applicable aux passeports et cartes d'identité

le Verwaltungsgericht Wiesbaden (tribunal administratif de Wiesbaden)
[OMISSIS]

a ordonné ce qui suit le 13 janvier 2022,

I. Il est sursis à statuer.

II. La procédure est déferée à la Cour de justice de l'Union européenne, conformément à l'article 267 TFUE, en vue d'une décision à titre préjudiciel sur les questions suivantes :

L'obligation relative à l'intégration et au stockage d'empreintes digitales dans les cartes d'identité, prévue à l'article 3, paragraphe 5, du 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 (JO 2019, L 188, p. 67), est-elle contraire à des normes de droit de l'Union de rang supérieur, en particulier

- a) **à l'article 77, paragraphe 3, TFUE**
- b) **aux articles 7 et 8 de la charte des droits fondamentaux de l'Union européenne**
- c) **à l'article 35, paragraphe 10, du RGPD**

et est-elle par conséquent invalide à l'un de ces titres ?

Motifs

I.

- 1 Le requérant sollicite la délivrance d'une carte d'identité qui n'intègre pas ses empreintes digitales. La défenderesse s'y oppose, au motif que l'article 5, paragraphe 9, du PAuswG [Gesetz über Personalausweise und den elektronischen Identitätsnachweis (loi sur les cartes d'identité et la preuve d'identité électronique)], qui a pour fondement le 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 (JO 2019, L 188, p. 67), impose d'intégrer deux empreintes digitales dans la carte d'identité.

- 2 Le règlement 2019/1157 est applicable depuis le 2 août 2021. Il est obligatoire dans tous ses éléments et directement applicable dans tout État membre. Aux termes de son article 3, paragraphe 5, les cartes d'identité délivrées par les États membres intègrent un support de stockage qui contient une image faciale du titulaire de la carte et deux empreintes digitales dans des formats numériques interopérables. Des dispositions de droit national ont également été adoptées aux fins de l'intégration des empreintes digitales dans les cartes d'identité (article 5, paragraphe 9, du PAuswG), le législateur national ayant considéré, ainsi que cela ressort de l'exposé des motifs de la loi (documents du Bundestag 19/21986, p. 22), que l'intégration des empreintes digitales s'imposait en vertu de l'article 3, paragraphe 5, du règlement 2019/1157.
- 3 Le 30 novembre 2021, le requérant a sollicité la délivrance d'une nouvelle carte d'identité sans empreintes digitales, la puce de son ancienne carte étant défectueuse. La nouvelle délivrance lui a été refusée au motif que, depuis le 2 août 2021, les cartes d'identité doivent obligatoirement intégrer des empreintes digitales. En outre, selon l'autorité compétente, le requérant n'avait pas droit à la délivrance d'une nouvelle carte d'identité puisqu'il était déjà en possession d'un document d'identité valable, une carte d'identité restant valable même si sa puce est défectueuse.
- 4 L'autorité compétente, en vertu du droit national, pour la délivrance des cartes d'identité agit en tant qu'autorité de sûreté conformément au droit de l'État membre. Cependant, la délivrance des cartes d'identité ainsi que le traitement des données associé à cette procédure ne relèvent justement pas de la directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil (également appelée « directive relative à la sûreté »), mais du [règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données)] ou RGPD (voir considérant 40 du règlement 2019/1157). En l'espèce, le maire n'intervient donc pas dans le domaine du droit européen de la sûreté, devant faire l'objet d'une interprétation autonome. Conformément à son article 1^{er}, paragraphe 1, et à son article 2, paragraphe 1, la directive 2016/680 ne s'applique que lorsque les autorités publiques interviennent à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la

prévention de telles menaces. Le système des passeports et des cartes d'identité n'en fait pas partie.

II.

1. Charte des droits fondamentaux de l'Union européenne (ci-après la « Charte »)

5 Article 7 de la Charte

« Respect de la vie privée et familiale

Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de ses communications. »

6 Article 8 de la Charte

Protection des données à caractère personnel

1. Toute personne a droit à la protection des données à caractère personnel la concernant.

2. Ces données doivent être traitées loyalement, à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi. Toute personne a le droit d'accéder aux données collectées la concernant et d'en obtenir la rectification.

3. Le respect de ces règles est soumis au contrôle d'une autorité indépendante.

7 Article 52 de la Charte

Portée et interprétation des droits et des principes

1. Toute limitation de l'exercice des droits et libertés reconnus par la présente Charte doit être prévue par la loi et respecter le contenu essentiel desdits droits et libertés. Dans le respect du principe de proportionnalité, des limitations ne peuvent être apportées que si elles sont nécessaires et répondent effectivement à des objectifs d'intérêt général reconnus par l'Union ou au besoin de protection des droits et libertés d'autrui.

2. Les droits reconnus par la présente Charte qui font l'objet de dispositions dans les traités s'exercent dans les conditions et limites définies par ceux-ci.

3. Dans la mesure où la présente Charte contient des droits correspondant à des droits garantis par la Convention européenne de sauvegarde des droits de l'Homme et des libertés fondamentales, leur sens et leur portée sont les mêmes que ceux que leur confère ladite convention. Cette disposition ne fait pas obstacle à ce que le droit de l'Union accorde une protection plus étendue.

4. Dans la mesure où la présente Charte reconnaît des droits fondamentaux tels qu'ils résultent des traditions constitutionnelles communes aux États membres, ces droits doivent être interprétés en harmonie avec lesdites traditions.

5. Les dispositions de la présente Charte qui contiennent des principes peuvent être mises en œuvre par des actes législatifs et exécutifs pris par les institutions, organes et organismes de l'Union, et par des actes des États membres lorsqu'ils mettent en œuvre le droit de l'Union, dans l'exercice de leurs compétences respectives. Leur invocation devant le juge n'est admise que pour l'interprétation et le contrôle de la légalité de tels actes.

6. Les législations et pratiques nationales doivent être pleinement prises en compte comme précisé dans la présente Charte.

7. Les explications élaborées en vue de guider l'interprétation de la présente Charte sont dûment prises en considération par les juridictions de l'Union et des États membres.

2. Traité sur le fonctionnement de l'Union européenne (TFUE) [OMISSIS].

8 Article 21 TFUE

[Libre circulation des personnes]

1. Tout citoyen de l'Union a le droit de circuler et de séjourner librement sur le territoire des États membres, sous réserve des limitations et conditions prévues par les traités et par les dispositions prises pour leur application.

2. Si une action de l'Union apparaît nécessaire pour atteindre cet objectif, et sauf si les traités ont prévu des pouvoirs d'action à cet effet, le Parlement européen et le Conseil, statuant conformément à la procédure législative ordinaire, peuvent arrêter des dispositions visant à faciliter l'exercice des droits visés au paragraphe 1.

3. Aux mêmes fins que celles visées au paragraphe 1, et sauf si les traités ont prévu des pouvoirs d'action à cet effet, le Conseil, statuant conformément à une procédure législative spéciale, peut arrêter des mesures concernant la sécurité sociale ou la protection sociale. Le Conseil statue à l'unanimité, après consultation du Parlement européen.

9 Article 77 TFUE

[Politique de gestion des frontières]

1. L'Union développe une politique visant :

a) à assurer l'absence de tout contrôle des personnes, quelle que soit leur nationalité, lorsqu'elles franchissent les frontières intérieures ;

b) à assurer le contrôle des personnes et la surveillance efficace du franchissement des frontières extérieures ;

c) à mettre en place progressivement un système intégré de gestion des frontières extérieures.

2. Aux fins du paragraphe 1, le Parlement européen et le Conseil, statuant conformément à la procédure législative ordinaire, adoptent les mesures portant sur :

a) la politique commune de visas et d'autres titres de séjour de courte durée ;

b) les contrôles auxquels sont soumises les personnes franchissant les frontières extérieures ;

c) les conditions dans lesquelles les ressortissants des pays tiers peuvent circuler librement dans l'Union pendant une courte durée ;

d) toute mesure nécessaire pour l'établissement progressif d'un système intégré de gestion des frontières extérieures ;

e) l'absence de tout contrôle des personnes, quelle que soit leur nationalité, lorsqu'elles franchissent les frontières intérieures.

3. Si une action de l'Union apparaît nécessaire pour faciliter l'exercice du droit, visé à l'article 20, paragraphe 2, point a), et sauf si les traités ont prévu des pouvoirs d'action à cet effet, le Conseil, statuant conformément à une procédure législative spéciale, peut arrêter des dispositions concernant les passeports, les cartes d'identité, les titres de séjour ou tout autre document assimilé. Le Conseil statue à l'unanimité, après consultation du Parlement européen.

4. Le présent article n'affecte pas la compétence des États membres concernant la délimitation géographique de leurs frontières, conformément au droit international.

10 Article 289 TFUE

[Procédures législatives ordinaire et spéciale ; droit d'initiative dans des cas spécifiques]

1. La procédure législative ordinaire consiste en l'adoption d'un règlement, d'une directive ou d'une décision conjointement par le Parlement européen et le Conseil, sur proposition de la Commission. Cette procédure est définie à l'article 294.

2. Dans les cas spécifiques prévus par les traités, l'adoption d'un règlement, d'une directive ou d'une décision par le Parlement européen avec la participation du Conseil ou par celui-ci avec la participation du Parlement européen constitue une procédure législative spéciale.

3. Les actes juridiques adoptés par procédure législative constituent des actes législatifs.

4. Dans les cas spécifiques prévus par les traités, les actes législatifs peuvent être adoptés sur initiative d'un groupe d'États membres ou du Parlement européen, sur recommandation de la Banque centrale européenne ou sur demande de la Cour de justice ou de la Banque européenne d'investissement.

3. 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 (JO L 188 du 12 juillet 2019, p. 67).

11 Considérant 2

La citoyenneté de l'Union confère à tout citoyen de l'Union le droit à la libre circulation sous réserve de certaines limitations et conditions. La directive 2004/38/CE du Parlement européen et du Conseil (3) donne effet à ce droit. L'article 45 de la Charte des droits fondamentaux de l'Union européenne (ci-après dénommée « Charte ») prévoit également la liberté de circulation et de séjour. La liberté de circulation implique le droit de sortir d'un État membre ou d'y entrer avec une carte d'identité ou un passeport en cours de validité.

12 Considérant 17

Les éléments de sécurité sont nécessaires pour vérifier l'authenticité d'un document et pour établir l'identité d'une personne. L'établissement de normes minimales de sécurité et l'intégration de données biométriques dans les cartes d'identité et les cartes de séjour des membres de la famille qui n'ont pas la nationalité d'un État membre sont des étapes importantes pour rendre leur utilisation dans l'Union plus sûre. L'ajout de tels éléments d'identification biométriques devrait permettre aux citoyens de l'Union de profiter pleinement de leurs droits à la libre circulation.

13 Considérant 18

Le stockage d'une image faciale et de deux empreintes digitales (ci-après dénommées « données biométriques ») sur les cartes d'identité et les cartes de séjour, comme cela est déjà prévu pour les passeports et titres de séjour biométriques des ressortissants de pays tiers, combine de manière appropriée une identification et une authentification fiables avec une réduction du risque de fraude, dans l'optique de renforcer la sécurité des cartes d'identité et des cartes de séjour.

14 Considérant 19

De manière générale, les États membres devraient, aux fins de la vérification de l'authenticité du document et de l'identité du titulaire, vérifier en priorité l'image faciale et, si nécessaire pour confirmer sans aucun doute l'authenticité du document et l'identité du titulaire, les États membres devraient également vérifier les empreintes digitales.

15 Considérant 21

Le présent règlement ne fournit pas de base juridique pour la création ou la tenue à jour de bases de données au niveau national pour le stockage de données biométriques dans les États membres, qui relève du droit national qui doit respecter le droit de l'Union en matière de protection des données. En outre, le présent règlement ne fournit pas de base juridique pour la création ou la tenue à jour d'une base de données centralisée au niveau de l'Union.

16 Considérant 22

Les éléments d'identification biométriques devraient être recueillis et stockés sur le support de stockage des cartes d'identité et des documents de séjour aux fins de la vérification de l'authenticité du document et de l'identité du titulaire. Une telle vérification ne devrait être effectuée que par du personnel dûment autorisé et uniquement lorsque la loi exige la présentation du document. En outre, les données biométriques stockées aux fins de la personnalisation des cartes d'identité ou des documents de séjour devraient être conservées de manière très sécurisée et uniquement jusqu'à la date de remise du document et, en tout état de cause, pas plus de 90 jours à compter de la date de délivrance du document. Après ce délai, ces données biométriques devraient être immédiatement effacées ou détruites. Cela devrait s'entendre sans préjudice de tout autre traitement de ces données conformément au droit de l'Union et au droit national en matière de protection des données.

17 Considérant 40

Le règlement (UE) 2016/679 du Parlement européen et du Conseil (9) s'applique en ce qui concerne les données à caractère personnel à traiter dans le cadre de l'application du présent règlement. Il est nécessaire de préciser davantage les garanties applicables aux données à caractère personnel traitées, et en particulier aux données sensibles, telles que les éléments d'identification biométriques. Les personnes concernées devraient être informées de l'existence, dans leurs documents, du support de stockage contenant leurs données biométriques, y compris de son accessibilité sous une forme sans contact, ainsi que de tous les cas où les données contenues dans leurs cartes d'identité et documents de séjour sont utilisées. En tout état de cause, les personnes concernées devraient avoir accès aux données à caractère personnel traitées dans leurs cartes d'identité et documents de séjour et devraient avoir le droit de les faire rectifier au moyen de la délivrance d'un nouveau document dans lequel ces données erronées ou

incomplètes sont corrigées ou complétées. Le support de stockage devrait être hautement sécurisé et les données à caractère personnel qu'il contient devraient être protégées efficacement contre l'accès non autorisé.

18 **Considérant 41**

Il convient que les États membres soient responsables du traitement correct des données biométriques, du recueil à l'intégration des données sur le support de stockage hautement sécurisé, conformément au règlement (UE) 2016/679.

19 **Article 3 du règlement 2019/1157**

Normes de sécurité/format/spécifications

1. Les cartes d'identité délivrées par les États membres sont de format ID-1 et comportent une zone de lecture automatique (ZLA). Ces cartes d'identité sont établies suivant les spécifications et les normes minimales de sécurité définies dans le document 9303 de l'OACI et respectent les exigences énoncées aux points c), d), f) et g) de l'annexe du règlement (CE) n° 1030/2002 tel qu'amendé par le règlement (UE) 2017/1954.

2. Les éléments de données figurant sur les cartes d'identité respectent les spécifications énoncées à la partie 5 du document 9303 de l'OACI.

Par dérogation au premier alinéa, le numéro du document peut être inséré dans la zone I et la désignation du genre de la personne est facultative.

3. Le document porte le titre « Carte d'identité » ou un autre intitulé national reconnu dans la ou les langues officielles de l'État membre de délivrance, ainsi que les mots « Carte d'identité » dans au moins une autre langue officielle des institutions de l'Union.

4. La carte d'identité comporte, au recto, le code pays à deux lettres de l'État membre délivrant la carte, imprimé en négatif dans un rectangle bleu et entouré de douze étoiles jaunes.

5. Les cartes d'identité intègrent un support de stockage hautement sécurisé qui contient une image faciale du titulaire de la carte et deux empreintes digitales dans des formats numériques interopérables. Pour le recueil des éléments d'identification biométriques, les États membres appliquent les spécifications techniques établies par la décision d'exécution C(2018)7767 de la Commission.

20 **Article 11 du règlement 2019/1157**

Protection des données à caractère personnel et responsabilité

1. Sans préjudice du règlement (UE) 2016/679, les États membres veillent à la sécurité, à l'intégrité, à l'authenticité et à la confidentialité des données recueillies et stockées aux fins du présent règlement.

2. Aux fins du présent règlement, les autorités chargées de la délivrance des cartes d'identité et des documents de séjour sont considérées comme le responsable du traitement visé à l'article 4, paragraphe 7, du règlement (UE) 2016/679 et sont responsables du traitement des données à caractère personnel.

3. Les États membres veillent à ce que les autorités de contrôle puissent exercer pleinement leurs missions visées dans le règlement (UE) 2016/679, y compris l'accès à toutes les données à caractère personnel et à toutes les informations nécessaires ainsi que l'accès à tout local ou matériel de traitement des données des autorités compétentes.

4. La coopération avec les prestataires de services extérieurs n'exclut pas la responsabilité d'un État membre qui peut découler du droit de l'Union ou du droit national en cas de manquement aux obligations en matière de données à caractère personnel.

5. Les informations lisibles par machine ne peuvent figurer sur une carte d'identité ou un document de séjour que conformément au présent règlement et au droit national de l'État membre de délivrance.

6. Les données biométriques stockées sur le support de stockage des cartes d'identité et des documents de séjour ne sont utilisées, conformément au droit de l'Union et au droit national, que par le personnel dûment autorisé des autorités nationales compétentes et des agences de l'Union pour vérifier :

a) l'authenticité de la carte d'identité ou du document de séjour ;

b) l'identité du titulaire grâce à des éléments comparables directement disponibles lorsque la loi exige la présentation de la carte d'identité ou du document de séjour.

7. Les États membres tiennent à jour et communiquent chaque année à la Commission la liste des autorités compétentes ayant accès aux données biométriques stockées sur le support de stockage visé à l'article 3, paragraphe 5, du présent règlement. La Commission publie en ligne une compilation de ces listes nationales.

4. Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données – RGPD ; JO du 4 mai 2016, L 119, p. 1).

21 Article 9 du règlement 2016/679

Traitement portant sur des catégories particulières de données à caractère personnel

1. Le traitement des données à caractère personnel qui révèle l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique sont interdits.

2. Le paragraphe 1 ne s'applique pas si l'une des conditions suivantes est remplie :

a) la personne concernée a donné son consentement explicite au traitement de ces données à caractère personnel pour une ou plusieurs finalités spécifiques, sauf lorsque le droit de l'Union ou le droit de l'État membre prévoit que l'interdiction visée au paragraphe 1 ne peut pas être levée par la personne concernée ;

b) le traitement est nécessaire aux fins de l'exécution des obligations et de l'exercice des droits propres au responsable du traitement ou à la personne concernée en matière de droit du travail, de la sécurité sociale et de la protection sociale, dans la mesure où ce traitement est autorisé par le droit de l'Union, par le droit d'un État membre ou par une convention collective conclue en vertu du droit d'un État membre qui prévoit des garanties appropriées pour les droits fondamentaux et les intérêts de la personne concernée ;

c) le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique, dans le cas où la personne concernée se trouve dans l'incapacité physique ou juridique de donner son consentement ;

d) le traitement est effectué, dans le cadre de leurs activités légitimes et moyennant les garanties appropriées, par une fondation, une association ou tout autre organisme à but non lucratif et poursuivant une finalité politique, philosophique, religieuse ou syndicale, à condition que ledit traitement se rapporte exclusivement aux membres ou aux anciens membres dudit organisme ou aux personnes entretenant avec celui-ci des contacts réguliers en liaison avec ses finalités et que les données à caractère personnel ne soient pas communiquées en dehors de cet organisme sans le consentement des personnes concernées ;

e) le traitement porte sur des données à caractère personnel qui sont manifestement rendues publiques par la personne concernée ;

f) le traitement est nécessaire à la constatation, à l'exercice ou à la défense d'un droit en justice ou chaque fois que des juridictions agissent dans le cadre de leur fonction juridictionnelle ;

g) le traitement est nécessaire pour des motifs d'intérêt public important, sur la base du droit de l'Union ou du droit d'un État membre qui doit être proportionné à l'objectif poursuivi, respecter l'essence du droit à la protection des données et prévoir des mesures appropriées et spécifiques pour la sauvegarde des droits fondamentaux et des intérêts de la personne concernée ;

h) le traitement est nécessaire aux fins de la médecine préventive ou de la médecine du travail, de l'appréciation de la capacité de travail du travailleur, de diagnostics médicaux, de la prise en charge sanitaire ou sociale, ou de la gestion des systèmes et des services de soins de santé ou de protection sociale sur la base du droit de l'Union, du droit d'un État membre ou en vertu d'un contrat conclu avec un professionnel de la santé et soumis aux conditions et garanties visées au paragraphe 3 ;

i) le traitement est nécessaire pour des motifs d'intérêt public dans le domaine de la santé publique, tels que la protection contre les menaces transfrontalières graves pesant sur la santé, ou aux fins de garantir des normes élevées de qualité et de sécurité des soins de santé et des médicaments ou des dispositifs médicaux, sur la base du droit de l'Union ou du droit de l'État membre qui prévoit des mesures appropriées et spécifiques pour la sauvegarde des droits et libertés de la personne concernée, notamment le secret professionnel ;

j) le traitement est nécessaire à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques, conformément à l'article 89, paragraphe 1, sur la base du droit de l'Union ou du droit d'un État membre qui doit être proportionné à l'objectif poursuivi, respecter l'essence du droit à la protection des données et prévoir des mesures appropriées et spécifiques pour la sauvegarde des droits fondamentaux et des intérêts de la personne concernée.

3. Les données à caractère personnel visées au paragraphe 1 peuvent faire l'objet d'un traitement aux fins prévues au paragraphe 2, point h), si ces données sont traitées par un professionnel de la santé soumis à une obligation de secret professionnel conformément au droit de l'Union, au droit d'un État membre ou aux règles arrêtées par les organismes nationaux compétents, ou sous sa responsabilité, ou par une autre personne également soumise à une obligation de secret conformément au droit de l'Union ou au droit d'un État membre ou aux règles arrêtées par les organismes nationaux compétents.

4. Les États membres peuvent maintenir ou introduire des conditions supplémentaires, y compris des limitations, en ce qui concerne le traitement des données génétiques, des données biométriques ou des données concernant la santé.

22 Article 35 du règlement 2016/679

1. Lorsqu'un type de traitement, en particulier par le recours à de nouvelles technologies, et compte tenu de la nature, de la portée, du contexte et des finalités du traitement, est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, le responsable du traitement effectue, avant le traitement, une analyse de l'impact des opérations de traitement envisagées sur la protection des données à caractère personnel. Une seule et même analyse peut

porter sur un ensemble d'opérations de traitement similaires qui présentent des risques élevés similaires.

[...]

10. Lorsque le traitement effectué en application de l'article 6, paragraphe 1, point c) ou e), a une base juridique dans le droit de l'Union ou dans le droit de l'État membre auquel le responsable du traitement est soumis, que ce droit règlemente l'opération de traitement spécifique ou l'ensemble des opérations de traitement en question et qu'une analyse d'impact relative à la protection des données a déjà été effectuée dans le cadre d'une analyse d'impact générale réalisée dans le cadre de l'adoption de la base juridique en question, les paragraphes 1 à 7 ne s'appliquent pas, à moins que les États membres n'estiment qu'il est nécessaire d'effectuer une telle analyse avant les activités de traitement.

5. [Gesetz über Personalausweise und den elektronischen Identitätsnachweis (loi sur les cartes d'identité et la preuve d'identité électronique)] Personalausweisgesetz (ci-après « PAuswG ») du 18 juin 2009 (BGBl. I p. 1346), modifiée en dernier lieu par l'article 2 de la loi du 5 juillet 2021 (BGBl. I p. 2281) [OMISSIS].

23 Article 5 du PAuswG

Modèle de carte d'identité ; données stockées

[...]

(9) Les deux empreintes digitales du demandeur [de carte d'identité] devant être conservées sur le support de stockage électronique en application du 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 (JO L 188 du 12 juillet 2019, p. 67) sont enregistrées sur le support de stockage et de traitement électronique de la carte d'identité sous la forme des empreintes à plat de l'index gauche et de l'index droit. Dans les cas d'absence d'index, de qualité insuffisante de l'empreinte digitale ou de blessure de la pulpe digitale, il conviendra d'y substituer l'empreinte à plat du pouce, du majeur ou de l'annulaire. Les empreintes digitales ne sont pas enregistrées lorsque le relevé des empreintes digitales est impossible pour des raisons médicales qui ne sont pas uniquement de nature temporaire.

24 Article 9 du PAuswG

Délivrance de la carte

(1) Les cartes d'identité ainsi que les cartes d'identité provisoires sont délivrées sur demande aux Allemands au sens de l'article 116, paragraphe 1, de la Loi

fondamentale. L'article 3a, paragraphe 1, du *Verwaltungsverfahrensgesetz* (loi sur la procédure administrative) n'est pas applicable. Les déclarations supplémentaires devant être fournies dans le cadre de la procédure de demande peuvent être effectuées au moyen d'un transfert de données. Le demandeur et son représentant légal ne peuvent se faire représenter par un mandataire lors du dépôt de la demande. Cette règle ne s'applique pas à un demandeur incapable d'agir ou de donner son consentement, lorsqu'une procuration spécifique certifiée ou authentifiée a été établie. Le demandeur et son représentant légal ou désigné doivent se présenter en personne.

(2) Pour les mineurs de moins de 16 ans ainsi que pour les personnes juridiquement incapables et qui ne sont pas représentées conformément au paragraphe 1, cinquième phrase, seule la personne qui dispose du droit de garde ou qui est en droit de déterminer leur lieu de résidence en tant que tuteur ou curateur peut introduire la demande. Elle est tenue d'introduire la demande de délivrance d'une carte d'identité concernant un mineur âgé d'au moins 16 ans mais de moins de 18 ans dans un délai de six semaines à compter de la date à laquelle l'intéressé atteint l'âge de 16 ans, si ce dernier omet de le faire. Les mineurs âgés d'au moins 16 ans sont autorisés à accomplir les démarches prévues par la présente loi.

(3) La demande doit indiquer tous les éléments nécessaires pour établir l'identité du demandeur et sa qualité d'Allemand. Les informations relatives au titre de docteur ainsi qu'aux noms d'Ordre et aux noms d'artiste sont facultatives. Il appartient au demandeur de fournir les preuves nécessaires. Les empreintes digitales des enfants ne sont pas relevées avant l'âge de six ans.

(4) En cas de doute sur l'identité du demandeur, il convient de prendre les mesures nécessaires pour établir son identité. L'autorité en charge de la délivrance des cartes d'identité peut faire procéder à des mesures d'identification si l'identité du demandeur ne peut être établie d'une autre manière ou seulement au prix de grandes difficultés. Une fois l'identité établie, les documents réunis aux fins d'établir l'identité doivent être détruits. Cette destruction doit faire l'objet d'un procès-verbal.

(5) La signature d'un enfant doit être apposée s'il est âgé d'au moins dix ans au moment de la demande de la carte d'identité.

(6) Pour les Allemands au sens de l'article 116, paragraphe 1, de la Loi fondamentale, des cartes d'identité de remplacement sont délivrées d'office conformément à l'article 6a. Les dispositions du paragraphe 1, deuxième à sixième phrases, du paragraphe 2, troisième phrase, du paragraphe 3, première à troisième phrases, et des paragraphes 4 et 5 s'appliquent mutatis mutandis.

III.

25 La juridiction de renvoi est habilitée à soumettre la question préjudicielle en application de l'article 267, premier alinéa, sous b), et deuxième alinéa, TFUE. En

effet, la question porte sur la validité de l'article 3, paragraphe 5, du règlement 2019/1157, un texte du droit dérivé de l'Union.

- 26 La réponse à cette question est nécessaire à la solution du litige. Si l'article 3, paragraphe 5, du règlement 2019/1157 est contraire à des dispositions de droit de l'Union de rang supérieur, le requérant a droit à la délivrance d'une carte d'identité qui n'intègre pas ses empreintes digitales, article 9, paragraphe 1, première phrase, du PAuswG. Les dispositions de droit national issues de l'article 5, paragraphe 9, du PAuswG n'auraient plus de fondement, car elles seraient contraires au droit de l'Union.
- 27 Même si l'ancienne carte d'identité du requérant reste valable malgré sa puce défectueuse, conformément à l'article 28, paragraphe 3, du PAuswG, le requérant doit se faire délivrer une nouvelle carte d'identité au plus tard à l'expiration de sa durée de validité, fixée à dix ans. En outre, en vertu de l'article 6, paragraphe 2, du PAuswG, le requérant peut demander une nouvelle carte d'identité avant l'expiration de la validité de la précédente s'il justifie d'un intérêt légitime à la nouvelle délivrance d'une carte. En cas de puce défectueuse, il n'est plus possible d'utiliser la fonction d'identification en ligne. Le contrôle automatisé aux frontières n'est plus utilisable non plus [OMISSIS]. Cette limitation des possibilités d'utilisation doit être considérée comme un intérêt légitime à une nouvelle délivrance.
- 28 Le tribunal de céans doute de la conformité de l'article 3, paragraphe 5, du règlement 2019/1175 avec le droit de l'Union. Ces doutes concernent l'application de la procédure législative ordinaire pour l'adoption du règlement 2019/1157, la question de la compatibilité de l'article 3, paragraphe 5, du règlement 2019/1157 avec les articles 7 et 8 de la Charte et l'absence de décision de mise en balance conformément à l'article 35, paragraphe 10, du RGPD.
- 29 1. Le tribunal de céans est convaincu que le règlement 2019/1157 aurait dû être adopté selon la procédure législative spéciale visée à l'article 77 TFUE.
- 30 L'article 289 TFUE distingue la procédure législative ordinaire et les procédures législatives spéciales. Le règlement 2019/1157 a pour base juridique l'article 21, paragraphe 2, TFUE et a été adopté sur proposition de la Commission européenne, après transmission du projet d'acte législatif aux parlements nationaux, avis du Comité économique et social européen et consultation du Comité des régions, conformément à la procédure législative ordinaire.
- 31 En vertu de l'article 21, paragraphe 2, TFUE, le Parlement européen et le Conseil, statuant conformément à la procédure législative ordinaire, peuvent arrêter des dispositions visant à faciliter l'exercice du droit de libre circulation si une action de l'Union apparaît nécessaire pour atteindre cet objectif, sauf si les traités ont prévu des pouvoirs d'action à cet effet.
- 32 L'article 77, paragraphe 3, première phrase, TFUE énonce une autre norme de compétence qui concerne notamment les règles relatives aux cartes d'identité. En

vertu de cette norme, le Conseil, statuant conformément à une procédure législative spéciale, peut arrêter des dispositions concernant les passeports, les cartes d'identité, les titres de séjour ou tout autre document assimilé – sauf si les traités ont prévu des pouvoirs d'action à cet effet – si une action de l'Union est nécessaire pour faciliter la libre circulation des personnes. Le Conseil statue à l'unanimité, après consultation du Parlement européen. Cette exigence d'unanimité laisse aux États membres la plus large souveraineté dans ce domaine [OMISSIS].

- 33 L'article 77 TFUE correspond à l'ancien article 62 TCE (traité CE). Pour le règlement (CE) 2252/2004 [du Conseil du 13 décembre 2004 établissant des normes pour les éléments de sécurité et les éléments biométriques intégrés dans les passeports et les documents de voyage délivrés par les États membres (JO L 385 du 29 décembre 2004, p. 1)], dont l'article 1^{er}, paragraphe 2, dispose que les empreintes digitales sont stockées dans les passeports, le législateur de l'époque avait choisi comme base juridique l'article 62 CE. Par un arrêt du 17 octobre 2013, la Cour a jugé que l'article 62, point 2, sous a), CE constituait une base juridique appropriée pour l'adoption du règlement (CE) n° 2252/2004, et notamment de son article 1^{er}, paragraphe 2 [arrêt du 17 octobre 2013, Schwarz (C-291/12, EU:C:2013:670, point 20)].
- 34 La compétence fondée sur l'article 77, paragraphe 3, TFUE prime sur l'article 21, paragraphe 2, TFUE, étant donné que l'article 77, paragraphe 3, TFUE, en tant que disposition plus spécifique de par son contenu, énonce des exigences plus élevées applicables à la procédure législative [OMISSIS] et que l'article 21, paragraphe 2, TFUE n'est pertinent que si les traités n'ont pas prévu de pouvoirs d'action pour atteindre l'objectif de promotion de la libre circulation. Le règlement 2019/1157 ne se réfère certes pas au développement de l'acquis de Schengen, mais, à l'instar du règlement 2252/2004, il vise l'harmonisation des éléments de sécurité et l'intégration d'éléments d'identification biométriques, en tant qu'étape importante vers l'utilisation de nouveaux éléments, dans la perspective d'évolutions ultérieures au niveau européen. L'objectif, de même qu'avec le règlement 2252/2004, est de renforcer la sécurité des documents (en l'occurrence les cartes d'identité et non les passeports).
- 35 Compte tenu de ces éléments, le tribunal de céans estime que le règlement 2019/1157 – et, partant, l'article 3, paragraphe 5, de celui-ci – n'aurait pu être valablement adopté que selon la procédure législative spéciale prévue à l'article 77, paragraphe 3, TFUE.
- 36 2. En outre, il existe des doutes matériels quant à la compatibilité avec les articles 7 et 8 de la Charte du recueil et du stockage d'empreintes digitales pour les cartes d'identité.
- 37 En vertu de l'article 7 de la Charte, toute personne a droit au respect de sa vie privée et familiale, de son domicile et de ses communications. Il découle de

l'article 8 de la Charte que toute personne a droit à la protection des données à caractère personnel la concernant.

- 38 Dès son arrêt du 17 octobre 2013, la Cour a constaté que le prélèvement et la conservation d'empreintes digitales par les autorités nationales, régis par l'article 1^{er}, paragraphe 2, du règlement n° 2252/2004, constituent une atteinte aux droits au respect de la vie privée et à la protection des données à caractère personnel [arrêt du 17 octobre 2013, Schwarz (C-291/12, EU:C:2013:670, point 30)]. Les empreintes digitales sont des données à caractère personnel, dès lors qu'elles contiennent objectivement des informations uniques sur des personnes physiques et permettent leur identification précise [arrêt du 17 octobre 2013, Schwarz (C-291/12, EU:C:2013:670, point 27), renvoyant à l'arrêt de la Cour EDH du 4 décembre 2008, S. et Marper c. Royaume-Uni, Recueil des arrêts et décisions 2008- V, p. 213, § 68 et 84)]. Les mêmes droits fondamentaux sont également affectés par le recueil et le stockage d'empreintes digitales pour les cartes d'identité.
- 39 Le tribunal de céans n'est pas certain que le recueil des empreintes digitales, et donc l'atteinte aux articles 7 et 8 de la Charte, soit également justifié pour les cartes d'identité.
- 40 Conformément à l'article 52, paragraphe 1, de la Charte, toute limitation de l'exercice des droits et libertés reconnus par la Charte doit être prévue par la loi et respecter le contenu essentiel desdits droits et libertés. Dans le respect du principe de proportionnalité, des limitations ne peuvent être apportées que si elles sont nécessaires et répondent effectivement à des objectifs d'intérêt général reconnus par l'Union ou au besoin de protection des droits et libertés d'autrui.
- 41 En outre, l'article 8, paragraphe 2, de la Charte dispose que les données à caractère personnel ne peuvent être traitées que sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi.
- 42 En l'espèce, le tribunal de céans est convaincu – de même que la Cour l'a jugé pour les passeports – que les personnes qui demandent une carte d'identité n'ont pas consenti au recueil de leurs empreintes digitales. Il ressort pourtant de l'article 3, paragraphe 5, du règlement 2019/1157 qu'il s'agit d'une disposition légale applicable à toutes les cartes d'identité.
- 43 Conformément à l'article 1^{er}, paragraphe 1, première phrase, du PAuswG, tous les Allemands sont tenus de posséder une carte d'identité valable dès qu'ils atteignent l'âge de 16 ans et sont soumis à l'obligation générale d'enregistrement ou, s'ils ne sont pas soumis à cette obligation, lorsqu'ils séjournent principalement en Allemagne. Le relevé des empreintes digitales est donc obligatoire pour la délivrance de ce document. Dès lors que la carte d'identité est obligatoire, il ne saurait être présumé que les personnes faisant la demande d'une carte d'identité ont consenti à un tel traitement de données [voir également en ce sens arrêt du 17 octobre 2013, Schwarz (C-291/12, EU:C:2013:670, point 31)].

- 44 Un fondement *légitime* prévu par la loi est donc nécessaire, conformément à l'article 52, paragraphe 1, de la Charte.
- 45 L'intégration des empreintes digitales dans les cartes d'identité est certes prévue par la loi, à l'article 3, paragraphe 5, du règlement 2019/1157. Cela répond également, du moins en partie, aux objectifs d'intérêt général reconnus par l'Union.
- 46 Selon ses considérants 1, 4 et 46, le règlement 2019/1157 vise à renforcer la libre circulation des personnes et à prévenir la falsification de documents ou la description fallacieuse d'un fait matériel concernant les conditions attachées au droit de séjour. La liberté de circulation implique le droit de sortir d'un État membre ou d'y entrer avec une carte d'identité ou un passeport en cours de validité (considérant 2). Selon le considérant 18, l'intégration des empreintes digitales a pour but de permettre, en combinaison avec l'image faciale, une identification fiable du titulaire et une réduction du risque de fraude.
- 47 Au sein de l'Union européenne, la carte d'identité peut être utilisée dans le cadre du franchissement des frontières. En outre, des États qui ne font pas partie de l'Union européenne autorisent également l'entrée sur leur territoire avec une carte d'identité, notamment la Suisse, l'Islande, la Norvège, l'Albanie et le Monténégro. Dans ces conditions, la carte d'identité est à tout le moins également utilisée comme document de voyage, de sorte que la réglementation sert également à empêcher l'entrée illégale en provenance de ces pays. Cela constituerait un objectif d'intérêt général reconnu par l'Union [arrêt du 17 octobre 2013, Schwarz (C-291/12, EU:C:2013:670, point 38)]. Cependant, l'objectif principal de la carte d'identité n'est justement pas, au premier chef, d'être un document de voyage, comme le passeport, dans l'espace Schengen. À cet égard, les considérants du règlement 2019/1157, contrairement à ceux du règlement 2252/2004, ne font justement pas référence à l'espace Schengen en tant qu'espace de liberté.
- 48 De même, ce n'est pas dans cette optique que le règlement 2019/1157 régit l'utilisation des données biométriques stockées : son article 11, paragraphe 6, prévoit que les données biométriques stockées ne sont utilisées que pour vérifier l'authenticité [du document] ou l'identité du titulaire. Le règlement 2019/1157 ne précise donc pas comment la libre circulation est censée être facilitée. L'objectif de prévention de l'entrée illégale ne peut en ce sens être assimilé au fait de faciliter la libre circulation.
- 49 Toutefois, même s'il y avait lieu de retenir que la réglementation poursuit un objectif d'intérêt général, des doutes subsistent quant à la proportionnalité de l'article 3, paragraphe 5, du règlement 2019/1157. Le principe de proportionnalité ne serait respecté que si les restrictions à ces droits issus de la Charte sont proportionnées au regard des buts poursuivis par le règlement 2019/1157 et, partant, au regard de l'objectif d'empêcher l'entrée illégale de personnes sur le territoire de l'Union et de permettre une identification fiable du titulaire de la

carte. À cet effet, les moyens mis en œuvre par ce règlement doivent être aptes à réaliser ces buts et ne pas aller au-delà de ce qui est nécessaire pour les atteindre [arrêt du 17 octobre 2013, Schwarz (C-291/12, EU:C:2013:670, points 40, 38)].

- 50 À cet égard, le tribunal de céans estime qu'il y a lieu de tenir compte du fait que la carte d'identité ne peut être assimilée au passeport, ni en fait ni en droit, mais qu'il existe des différences marquées dans l'utilisation de ces documents. L'article 3, paragraphe 5, du règlement 2019/1157 traite cependant les deux documents de la même manière en ce qui concerne les empreintes digitales.
- 51 S'il est vrai que la carte d'identité peut également être utilisée comme document de voyage, comme nous l'avons déjà exposé plus haut, il n'en reste pas moins que les cartes d'identité et les passeports diffèrent tant sur le plan juridique que sur le plan pratique. Même si les cartes d'identité sont également utilisées comme documents de voyage dans le contexte de la libre circulation, aucun contrôle de routine n'est effectué, du moins pour les voyages entre États membres de l'Union. En outre, pour la plupart des citoyens de l'Union, la fonction première de la carte nationale d'identité nationale n'est certainement pas liée à la libre circulation. L'usage de la carte d'identité est en effet loin d'être cantonné à cette seule fonction. Les cartes d'identité sont ainsi utilisées au quotidien, entre autres, dans le cadre des relations avec les autorités administratives nationales ou avec des personnes privées tierces, tels que des banques ou des compagnies aériennes. Les citoyens de l'Union qui souhaiteraient exercer leur liberté de circulation peuvent déjà le faire avec leur passeport (voir également en ce sens : Avis 7/2018 du Contrôleur européen de la protection des données (ci-après le « CEPD ») [sur la proposition de règlement relatif au renforcement de la sécurité des cartes d'identité des citoyens de l'Union et d'autres documents] du 10 août 2018, se prononçant sur la proposition visant à intégrer les empreintes digitales dans les cartes d'identité, disponible à l'adresse https://edps.europa.eu/sites/edp/files/publication/18-08-10_opinion_eid_fr.pdf [OMISSIS]) (ci-après l'« avis 7/2018 du CEPD »).
- 52 En outre, la détention d'une carte d'identité est obligatoire en Allemagne, selon l'article 1^{er}, paragraphe 1, première phrase, du PAuswG. Contrairement au passeport, le citoyen ne peut pas décider lui-même de demander ou non une carte d'identité. Le CEPD estime lui aussi que le fait d'intégrer et de stocker des empreintes digitales aurait une incidence considérable, touchant jusqu'à 370 millions de citoyens de l'Union et soumettant potentiellement 85 % de la population de l'Union au relevé obligatoire d'empreintes digitales. Cette large portée, conjuguée au caractère très sensible des données traitées (images faciales combinées à des empreintes digitales), appelle un examen attentif selon un critère de nécessité strict (avis 7/2018 du CEPD [OMISSIS]). Le tribunal de céans souscrit à l'affirmation du CEPD selon laquelle, compte tenu des différences entre les cartes d'identité et les passeports, l'introduction dans les cartes d'identité d'éléments de sécurité pouvant être considérés comme appropriés dans le cas des passeports ne peut être automatique, mais exige une réflexion et une analyse approfondie ([Résumé de l'avis du contrôleur européen de la protection des

données sur la proposition de règlement relatif au renforcement de la sécurité des cartes d'identité des citoyens de l'Union et d'autres documents] JO C 338 du 21 septembre 2018, p. 22). Celle-ci fait en l'espèce défaut.

- 53 Le tribunal de céans estime que les possibilités d'utilisation étendues décrites plus haut, combinées au grand nombre de citoyens de l'Union concernés, impliquent que le degré de l'ingérence est beaucoup plus élevé que pour les passeports, ce qui exige en contrepartie une justification plus forte.
- 54 Dans le cadre de l'interprétation des articles 7 et 8 de la Charte, il convient également de tenir compte des appréciations qui ressortent du RGPD. Selon les considérants 1 et 2 du RGPD, la protection des personnes physiques à l'égard du traitement des données à caractère personnel est un droit fondamental. Les principes et les règles régissant la protection des personnes physiques à l'égard du traitement des données à caractère personnel les concernant devraient, quelle que soit la nationalité ou la résidence de ces personnes physiques, respecter leurs libertés et droits fondamentaux, en particulier leur droit à la protection des données à caractère personnel. Le RGPD vise à contribuer à la réalisation d'un espace de liberté, de sécurité et de justice et d'une union économique, au progrès économique et social, à la consolidation et à la convergence des économies au sein du marché intérieur, ainsi qu'au bien-être des personnes physiques.
- 55 Les données dactyloscopiques relèvent d'un type particulier de données à caractère personnel au sens de l'article 9, paragraphe 1, du RGPD, à savoir les données biométriques. L'article 4, point 14, du RGPD définit les données biométriques comme 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. Conformément à l'article 9, paragraphe 1, du RGPD, le traitement de ces données biométriques est en principe interdit et n'est autorisé que dans des cas exceptionnels et strictement limités.
- 56 S'agissant de la protection contre la falsification à laquelle est censée contribuer l'intégration des empreintes digitales dans les cartes d'identité, il y a lieu d'observer qu'entre 2013 et 2017, seuls 38 870 cas de cartes d'identité frauduleuses auraient été constatés et que l'utilisation de cartes d'identité frauduleuses est en baisse depuis plusieurs années (avis 7/2018 du CEPD [OMISSIS]).
- 57 Le fait est qu'il n'est pas suffisamment certain que l'intégration des empreintes digitales dans les cartes d'identité puisse contribuer réellement à leur caractère infalsifiable. Une correspondance entre les données biométriques stockées dans la puce de la carte d'identité et les empreintes digitales du titulaire du document confirme uniquement que le document appartient à son titulaire. Cette concordance ne constitue pas en soi une preuve d'identité, tant que l'authenticité de la carte d'identité elle-même n'a pas également été établie. Il est certes reconnu

que l'utilisation de données biométriques réduit le risque qu'un document puisse effectivement être falsifié, de sorte que l'intégration des empreintes digitales peut, en partie au moins, contribuer à cet objectif (avis 7/2018 du CEPD [OMISSIS]).

- 58 Il semble toutefois extrêmement douteux que cette possibilité puisse justifier l'ampleur de l'ingérence, d'autant plus qu'en vertu du droit national, contrairement au règlement 2019/1157, même une carte d'identité dont la puce est défectueuse reste valable. À cet égard, selon les explications du Bundesamt für Sicherheit in der Informationstechnik (Office fédéral allemand pour la sécurité en matière de technologies de l'information) « une carte d'identité dont la puce ne fonctionne plus [conserve] sa validité, même si la puce intégrée est visiblement défectueuse. La sécurité en tant que document d'identité est assurée par les éléments de sécurité physiques » [OMISSIS]. Cependant, si ces éléments physiques (notamment les micro-impressions, les surimpressions réactives aux UV, etc.) suffisent pour établir la sécurité, la question de la nécessité d'intégrer les empreintes digitales se pose avec d'autant plus d'acuité.
- 59 Le CEPD a également souligné que les mesures de sécurité relatives à l'impression du document, telles que l'utilisation d'hologrammes ou de filigranes, étaient nettement moins intrusives. Ces méthodes n'impliqueraient pas le traitement de données à caractère personnel tout en permettant également d'empêcher la falsification des documents d'identité et de vérifier l'authenticité d'un document (avis 7/2018 du CEPD [OMISSIS]).
- 60 Dans ce cadre, il y a lieu également de respecter l'un des principes les plus importants du droit européen de la protection des données : celui de minimisation des données. En vertu de ce principe, le prélèvement et l'utilisation de données à caractère personnel doivent être adéquats, pertinents et limités à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées.
- 61 S'il s'avère nécessaire de recueillir les empreintes digitales, on peut également s'interroger sur la nécessité de capturer l'image de l'empreinte complète. Cela permet certes de favoriser l'interopérabilité des différents types de systèmes capables de reconnaître les empreintes digitales. Ces systèmes peuvent être classés en trois sous-catégories. D'une part, il existe des systèmes qui stockent et comparent des images complètes des empreintes digitales. D'autres systèmes utilisent ce qu'il convient d'appeler les minuties (points caractéristiques), à savoir un sous-ensemble de caractéristiques extraites des images des empreintes digitales. La troisième catégorie est celle des systèmes fonctionnant avec des motifs extraits des images d'empreintes digitales. Si seules les minuties étaient stockées, un État membre utilisant un système fonctionnant à partir d'une image de l'empreinte digitale complète ne pourrait pas les utiliser. Le stockage de l'intégralité de l'empreinte digitale favorise l'interopérabilité, mais accroît la quantité de données personnelles stockées et donc le risque d'usurpation d'identité en cas de fuite de données (avis 7/2018 du CEPD [OMISSIS]).

- 62 Les puces RFID utilisées dans les cartes d'identité peuvent, dans certaines circonstances, être lues par des scanners non autorisés. En effet, elles sont activées par un champ radioélectrique, les données étant ensuite transmises sous une forme chiffrée. La sécurité de la procédure dépend donc en définitive de la qualité de la technologie de transmission et de chiffrement. C'est précisément l'utilisation de l'empreinte digitale complète qui induit dans ce contexte une augmentation des risques [OMISSIS].
- 63 En tout état de cause, il faut également tenir compte du fait que les empreintes digitales sont des données biométriques. Le législateur a montré, notamment en adoptant l'article 9 du RGPD, que ces données font l'objet d'une protection particulière.
- 64 Même le règlement 2019/1157 renonce à l'« élément de sécurité » que constitue l'empreinte digitale pour les enfants de moins de 12 ans et exempte totalement les enfants de moins de 6 ans de l'obligation de relevé d'empreintes (article 3, paragraphe 7, du règlement 2019/1157). L'exemption de relevé qui est toutefois beaucoup plus significative est celle concernant les personnes pour lesquelles le prélèvement des empreintes digitales est physiquement impossible (par exemple en cas d'adématoglyphie). Le règlement 2019/1157 reste muet sur les éventuelles autres finalités de cet élément de sécurité, qui restent donc indéterminées.
- 65 **3.** Dans son avis du 10 août 2018, le CEPD souligne en outre que l'article 35, paragraphe 10, du RGPD s'applique à l'enrôlement et au traitement des empreintes digitales. En vertu de l'article 35, paragraphe 1, du RGPD, une analyse d'impact relative à la protection des données doit être effectuée avant tout traitement susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques. Cette analyse d'impact sur la protection des données devrait notamment comprendre une évaluation des risques pour les droits et libertés des personnes concernées, ainsi que les mesures envisagées pour faire face à ces risques, telles que des garanties et mesures de sécurité (avis 7/2018 du CEPD).
- 66 Étant donné que la base juridique est fondée sur des dispositions de droit de l'Union auxquelles le responsable du traitement est soumis et que celles-ci régissent l'opération de traitement spécifique, l'analyse d'impact générale doit être réalisée dans le cadre de l'adoption de cette base juridique (article 35, paragraphe 10, du règlement général sur la protection des données). Une telle analyse d'impact aurait donc dû être réalisée lors de l'adoption du règlement 2019/1157. Il ressort des considérants de celui-ci que cela n'a pas été le cas.
- 67 Le tribunal de céans estime, comme le CEPD dans son avis du 10 août 2018, que l'analyse d'impact ne permettrait pas de soutenir le choix de l'intégration obligatoire, dans la carte d'identité, de l'image faciale et des (deux) empreintes digitales. Au cours de la procédure législative, le CEPD a déjà recommandé de réévaluer la nécessité et la proportionnalité du traitement des données

biométriques (image faciale combinée aux empreintes digitales) dans ce cadre (JO 2018, C 338, p. 22).

- 68 Dans le considérant 40, le législateur n’aborde cette problématique que de manière très générale en ce qui concerne le RGPD. Il s’en tient à des affirmations imprécises, comme le fait que les citoyens de l’Union devraient être informés du support de stockage et qu’il faudrait préciser davantage les garanties applicables aux données à caractère personnel traitées, et en particulier aux données sensibles, telles que les éléments d’identification biométriques. Le support de stockage devrait être hautement sécurisé et les données à caractère personnel qu’il contient devraient être protégées efficacement contre l’accès non autorisé. Le règlement reste vague sur ce qu’il convient d’entendre par « hautement sécurisé » et sur la manière dont les garanties et les mesures de protection doivent être conçues. En particulier, il n’en ressort aucune mise en balance tenant compte des risques liés à une fuite des données de la puce et de l’atteinte aux articles 7 et 8 de la Charte.
- 69 La question se pose donc de savoir si le fait de ne pas avoir respecté l’obligation d’étude d’impact des risques peut rester sans incidence sur la validité d’une norme ou si le non-respect, par le législateur, de son obligation impérative de procéder à une étude d’impact ne devrait pas plutôt être sanctionné par l’invalidité de cette norme. À défaut, le législateur serait récompensé pour ses manquements.
- 70 Il s’ensuit qu’il est nécessaire de saisir la Cour afin d’obtenir des éclaircissements sur la validité de l’article 3, paragraphe 5, du règlement 2019/1157.

[OMISSIS]