Recueil de la jurisprudence

CONCLUSIONS DE L'AVOCATE GÉNÉRALE
M^ME LAILA MEDINA
présentées le 29 juin 2023 [1]

Affaire C-61/22

RL
contre
Landeshauptstadt Wiesbaden

[demande de décision préjudicielle formée par le Verwaltungsgericht Wiesbaden (tribunal administratif de Wiesbaden, Allemagne)]

« Renvoi préjudiciel – Règlement (UE) 2019/1157 – Renforcement de la sécurité des cartes d'identité des citoyens de l'Union – Article 3, paragraphe 5 – Obligation de recueillir des empreintes digitales et de les stocker sur un support de stockage hautement sécurisé – Validité – Base juridique – Article 21, paragraphe 2, TFUE – Article 77, paragraphe 3, TFUE – Charte des droits fondamentaux de l'Union européenne – Articles 7 et 8 – Respect de la vie privée et familiale – Protection des données à caractère personnel – Article 52, paragraphe 1 – Principe de proportionnalité – Règlement général sur la protection des données – Article 35, paragraphe 10 – Analyse d'impact relative à la protection des données »

I. Introduction

1. La présente demande de décision préjudicielle porte sur la validité de l'article 3, paragraphe 5, du règlement (UE) 2019/1157 [2], qui prévoit l'obligation d'intégrer, sur un support de stockage hautement sécurisé, une image des empreintes digitales du titulaire dans toute carte d'identité nouvellement délivrée par les États membres [3]. Cette demande a été présentée dans le cadre d'un litige opposant RL au Landeshauptstadt Wiesbaden (Wiesbaden, capitale du Land de Hesse, Allemagne) au sujet d'une décision administrative par laquelle cette dernière a refusé de délivrer une carte d'identité qui n'avait pas une empreinte digitale stockée dans sa puce.

2. Par sa demande, la juridiction de renvoi souhaite savoir, premièrement, si le fondement approprié pour l'adoption du règlement 2019/1157 était l'article 21, paragraphe 2, TFUE, deuxièmement, si l'article 3, paragraphe 5, de ce règlement est compatible avec les articles 7 et 8 de la charte des droits fondamentaux de l'Union européenne (ci-après la « Charte »), lus en

[1] Langue originale : l'anglais.

[2] Règlement 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).

[3] Cette obligation est applicable à partir du 2 août 2021. Voir article 16 du règlement 2019/1157.

combinaison avec l'article 52, paragraphe 1, de celle-ci et, troisièmement, si ledit règlement est conforme à l'obligation de procéder à une analyse d'impact relative à la protection des données prévue par l'article 35, paragraphe 10, du règlement (UE) 2016/679 [4].

3. Nonobstant les différences existantes entre les cartes d'identité et les passeports, la présente affaire constitue une extension thématique de l'arrêt Schwarz [5]. Dans cet arrêt, la Cour a examiné la validité de l'article 1er, paragraphe 2, du règlement (CE) nº 2252/2004 [6], qui prévoit le recueil et le stockage obligatoires d'empreintes digitales sur les passeports et autres documents de voyage délivrés par les États membres [7].

II. Le cadre juridique

A. Le droit de l'Union

1. Le règlement 2019/1157

4. Les considérants 1, 2, 3, 4, 5, 15, 17, 18, 21 et 28 du règlement 2019/1157 énoncent :

« (1) Le traité sur l'Union européenne souligne la détermination des États membres à faciliter la libre circulation des personnes, tout en assurant la sûreté et la sécurité de leurs peuples, en établissant un espace de liberté, de sécurité et de justice, conformément aux dispositions du traité sur l'Union européenne et du traité sur le fonctionnement de l'Union européenne.

(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] [8] donne effet à ce droit. L'article 45 de la [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.

(3) En vertu de la [directive 2004/38], les États membres doivent délivrer et renouveler les cartes d'identité ou les passeports de leurs ressortissants conformément à leur législation nationale [...]

(4) La [directive 2004/38] prévoit que les États membres peuvent adopter les mesures nécessaires pour refuser, annuler ou retirer tout droit conféré par ladite directive en cas d'abus de droit ou de fraude. La falsification de documents ou la description fallacieuse d'un fait matériel concernant les conditions attachées au droit de séjour ont été identifiées comme des cas typiques de fraude dans le cadre de cette directive.

[4] Règlement 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) (JO 2016, L 119, p. 1) (ci-après le « RGPD »).

[5] Arrêt du 17 octobre 2013 (C-291/12, ci-après l'« arrêt Schwarz », EU:C:2013:670).

[6] Règlement 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 2004, L 385, p. 1).

[7] La présente affaire est aussi étroitement liée à l'affaire C-280/22, Kinderrechtencoalitie Vlaanderen et Liga voor Mensenrechten, pendante devant la Cour.

[8] Directive du Parlement européen et du Conseil du 29 avril 2004 relative au droit des citoyens de l'Union et des membres de leurs familles de circuler et de séjourner librement sur le territoire des États membres, modifiant le règlement (CEE) nº 1612/68 et abrogeant les directives 64/221/CEE, 68/360/CEE, 72/194/CEE, 73/148/CEE, 75/34/CEE, 75/35/CEE, 90/364/CEE, 90/365/CEE et 93/96/CEE (JO 2004, L 158, p. 77), telle que modifiée.

(5) Des différences considérables existent entre les niveaux de sécurité des cartes nationales d'identité délivrées par les États membres et des documents de séjour des ressortissants de l'Union résidant dans un autre État membre et des membres de leur famille. Ces différences augmentent le risque de falsification et de fraude documentaire et entraînent également des difficultés pratiques pour les citoyens lorsqu'ils cherchent à exercer leur droit à la libre circulation [...]

[...]

(15) [...] L'amélioration des cartes d'identité devrait viser à faciliter l'identification et à contribuer à avoir un meilleur accès aux services.

[...]

(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 des données biométriques dans les cartes d'identité [...] 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.

(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.

[...]

(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.

[...]

(28) L'introduction de normes minimales en matière de sécurité et de format pour les cartes d'identité devrait permettre aux États membres de s'appuyer sur l'authenticité de ces documents lorsque les citoyens de l'Union exercent leur droit à la libre circulation. L'introduction de normes de sécurité renforcées devrait offrir des garanties suffisantes aux autorités publiques et aux entités privées pour leur permettre de se fier à l'authenticité des cartes d'identité lorsqu'elles sont utilisées par les citoyens de l'Union à des fins d'identification. »

5. L'article 1^er du règlement 2019/1157, intitulé « Objet », dispose :

« Le présent règlement renforce les normes de sécurité applicables aux cartes d'identité délivrées par les États membres à leurs ressortissants [...] lorsqu'ils exercent leur droit à la libre circulation. »

6. L'article 3 du règlement 2019/1157, intitulé « Normes de sécurité/format/spécifications », dispose :

« 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'[Organisation de l'aviation civile internationale (OACI)] et respectent les exigences énoncées aux points c), d), f) et g) de l'annexe du règlement (CE) nº 1030/2002 [du Conseil, du 13 juin 2002, établissant un modèle uniforme de titre de séjour pour les ressortissants de pays tiers (JO 2002, L 157, p. 1)] tel qu'amendé par le règlement (UE) 2017/1954 [du Parlement européen et du Conseil, du 25 octobre 2017 (JO 2017, L 286, p. 9)].

[...]

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 [9].

6. Le support de stockage a une capacité suffisante pour garantir l'intégrité, l'authenticité et la confidentialité des données. Les données stockées sont accessibles sous forme sans contact et sécurisées comme le prévoit la décision d'exécution C(2018) 7767 [de la Commission]. Les États membres échangent les informations nécessaires pour authentifier le support de stockage ainsi que pour consulter et vérifier les données biométriques visées au paragraphe 5.

7. Les enfants de moins de douze ans peuvent être exemptés de l'obligation de donner leurs empreintes digitales.

Les enfants de moins de six ans sont exemptés de l'obligation de donner leurs empreintes digitales.

Les personnes dont il est physiquement impossible de relever les empreintes digitales sont exemptées de l'obligation de les donner.

[...] »

7. L'article 10 du règlement 2019/1157, intitulé « Recueil d'éléments d'identification biométriques », dispose :

« 1. Les éléments d'identification biométriques sont recueillis exclusivement par du personnel qualifié et dûment habilité désigné par les autorités chargées de délivrer les cartes d'identité ou les cartes de séjour, dans le but d'être intégrés sur le support de stockage hautement sécurisé visé à l'article 3, paragraphe 5, pour les cartes d'identité [...]

Afin de garantir la cohérence des éléments d'identification biométriques avec l'identité du demandeur, ce dernier doit se présenter en personne au moins une fois au cours du processus de délivrance pour chaque demande.

9 Décision d'exécution du 30 novembre 2018 établissant les spécifications techniques du modèle uniforme de titre de séjour pour les ressortissants de pays tiers, et abrogeant la décision C(2002) 3069 [(2018) 7767 final] (ci-après la « décision C(2018) 7767 de la Commission »).

2. Les États membres veillent à ce que des procédures appropriées et efficaces soient en place pour le recueil des éléments d'identification biométriques et que ces procédures respectent les droits et les principes énoncés dans la Charte, la convention [européenne] de sauvegarde des droits de l'homme et des libertés fondamentales [signée à Rome le 4 novembre 1950, ci-après la « CEDH »] et la convention des Nations unies relative aux droits de l'enfant.

[...]

3. Sauf s'ils sont nécessaires aux finalités du traitement dans le respect du droit de l'Union et du droit national, les éléments d'identification biométriques stockés aux fins de la personnalisation des cartes d'identité ou des documents de séjour sont conservés 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 éléments d'identification biométriques sont immédiatement effacés ou détruits. »

8. L'article 11 du règlement 2019/1157, intitulé « Protection des données à caractère personnel et responsabilité », est libellé comme suit :

« 1. Sans préjudice du [RGPD], 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, [point] 7, du [RGPD] 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 [RGPD], 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.

[...]

5. Les informations lisibles par machine ne peuvent figurer sur une carte d'identité [...] 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.

[...] »

2. Le RGPD

9. L'article 6 du RGPD, intitulé « Licéité du traitement », est libellé comme suit :

« 1. Le traitement n'est licite que si, et dans la mesure où, au moins une des conditions suivantes est remplie :

[...]

c) le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis ;

d) le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique ;

e) le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement ;

[...] »

10. L'article 35 du RGPD, intitulé « Analyse d'impact relative à la protection des données », dispose :

« 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, [sous] 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 réglemente 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. »

3. La directive 2004/38

11. L'article 4 de la directive 2004/38, intitulé « Droit de sortie », dispose :

« 1. Sans préjudice des dispositions concernant les documents de voyage, applicables aux contrôles aux frontières nationales, tout citoyen de l'Union muni d'une carte d'identité ou d'un passeport en cours de validité ainsi que les membres de sa famille qui n'ont pas la nationalité

d'un État membre munis d'un passeport en cours de validité ont le droit de quitter le territoire d'un État membre en vue de se rendre dans un autre État membre.

[...] »

12. L'article 5 de la directive 2004/38, intitulé « Droit d'entrée », énonce :

« 1. Sans préjudice des dispositions concernant les documents de voyage, applicables aux contrôles aux frontières nationales, les États membres admettent sur leur territoire le citoyen de l'Union muni d'une carte d'identité ou d'un passeport en cours de validité ainsi que les membres de sa famille qui n'ont pas la nationalité d'un État membre et qui sont munis d'un passeport en cours de validité.

[...] »

B. Le droit allemand

13. Le Gesetz über Personalausweise und den elektronischen Identitätsnachweis (loi sur les cartes d'identité et la preuve électronique d'identité) [10] transpose en droit allemand l'obligation prévue à l'article 3, paragraphe 5, du règlement 2019/1157.

14. L'article 1er, paragraphe 1, du PAuswG, intitulé « Obligation d'identification ; droit d'identification », dispose :

« Les Allemands tels que définis à l'article 116, paragraphe 1, de la Loi fondamentale sont tenus de posséder une carte d'identité 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. Ils doivent présenter leur carte d'identité à la demande d'une autorité habilitée à vérifier l'identification. Les titulaires de cartes d'identité ne peuvent être tenus de déposer leur carte d'identité ou de la remettre d'une autre manière. Ce qui précède ne s'applique pas aux autorités habilitées à vérifier l'identification ni en cas de retrait ou de confiscation. »

15. L'article 5, paragraphe 9, du PAuswG, intitulé « Délivrance de la carte d'identité », dispose :

« Les deux empreintes digitales du demandeur devant être stockées sur le support de stockage électronique en application du [règlement 2019/1157], 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. »

[10] Loi 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, ci-après le « PAuswG »).

III. Le litige au principal et la question préjudicielle

16. Au mois de novembre 2021, RL a demandé à la capitale du Land de Hesse, Wiesbaden, la délivrance d'une nouvelle carte d'identité, en faisant valoir que la puce de son ancienne carte d'identité était défectueuse. Dans sa demande, RL a précisé qu'il souhaitait que cette carte soit délivrée sans qu'une image des empreintes digitales soit intégrée dans la puce.

17. La capitale du Land de Hesse, Wiesbaden, a rejeté la demande de RL au motif, d'une part, que, selon le droit allemand, une carte d'identité reste valable même si sa puce est défectueuse. Étant donné que RL était déjà en possession d'un document d'identité valable, il n'avait pas droit à la délivrance d'une nouvelle carte d'identité. D'autre part, la capitale du Land de Hesse, Wiesbaden, a considéré que, en tout état de cause, la carte d'identité ne pouvait être délivrée sans l'image des empreintes digitales du titulaire, étant donné que, depuis le 2 août 2021, il était devenu obligatoire, au titre de l'article 5, paragraphe 9, du PAuswG, de stocker une image des empreintes digitales dans la puce des nouvelles cartes d'identité.

18. RL a saisi le Verwaltungsgericht Wiesbaden (tribunal administratif de Wiesbaden, Allemagne), la juridiction de renvoi dans la présente affaire, d'un recours tendant à ce qu'il soit enjoint à l'autorité compétente de lui délivrer une nouvelle carte d'identité dans laquelle n'est pas stockée l'image de ses empreintes digitales.

19. La juridiction de renvoi nourrit des doutes quant à la validité de l'article 3, paragraphe 5, du règlement 2019/1157, qui constitue le fondement de l'article 5, paragraphe 9, du PAuswG et, partant, du caractère obligatoire du recueil et du stockage d'empreintes digitales dans les cartes d'identité allemandes. À cet égard, cette juridiction rappelle que, selon l'article 3, paragraphe 5, de ce règlement, les cartes d'identité délivrées par les États membres doivent intégrer un support de stockage hautement sécurisé qui contient une image faciale du titulaire de la carte ainsi que deux empreintes digitales dans des formats numériques interopérables.

20. En particulier, la juridiction de renvoi avance trois motifs d'invalidité de l'article 3, paragraphe 5, du règlement 2019/1157.

21. Premièrement, la juridiction de renvoi se demande si le règlement 2019/1157 aurait dû être adopté sur le fondement de l'article 77, paragraphe 3, TFUE, qui prévoit l'application d'une procédure législative spéciale dans le cadre de laquelle le Conseil statue à l'unanimité, plutôt que sur le fondement de l'article 21, paragraphe 2, TFUE, relatif à la procédure législative ordinaire, impliquant la codécision du Parlement européen et du Conseil de l'Union européenne. La juridiction de renvoi souligne que, dans l'arrêt Schwarz, la Cour a considéré que l'article 62, point 2, sous a), TCE, c'est-à-dire la disposition qui est devenue par la suite l'article 77, paragraphe 3, TFUE, constituait une base juridique appropriée pour l'adoption du règlement n° 2252/2004, qui prescrit le recueil et le stockage obligatoires d'empreintes digitales des citoyens de l'Union pour les passeports. Cette juridiction se demande donc si la même base juridique aurait dû être retenue pour l'adoption du règlement 2019/1157.

22. Deuxièmement, la juridiction de renvoi a des doutes quant à la compatibilité de l'article 3, paragraphe 5, du règlement 2019/1157 avec les articles 7 et 8 de la Charte. Cette juridiction relève que le recueil et le stockage obligatoires d'empreintes digitales pour les cartes d'identité constituent, au regard de l'arrêt Schwarz, une atteinte aux droits reconnus par ces deux dispositions. En outre, selon ladite juridiction, cette atteinte ne remplirait pas les conditions énoncées à l'article 8, paragraphe 2, et à l'article 52, paragraphe 1, de la Charte et ne serait donc pas

justifiée. Plus précisément, la juridiction de renvoi remet en cause le fait que l'article 3, paragraphe 5, du règlement 2019/1157 poursuit un intérêt légitime et que l'obligation découlant de cette disposition puisse être considérée comme appropriée, nécessaire et proportionnée.

23. Troisièmement, la juridiction de renvoi exprime des préoccupations quant à l'obligation de procéder à une analyse d'impact relative à la protection des données, prévue à l'article 35, paragraphe 10, du RGPD. En particulier, cette juridiction relève, en se référant à l'avis émis par le Contrôleur européen de la protection des données (CEPD) sur la proposition de règlement [11], que cette disposition s'applique au traitement des empreintes digitales prévu par le règlement 2019/1157. Or, une telle évaluation n'aurait pas été effectuée par le législateur de l'Union lors de l'adoption de ce règlement.

24. Dans ces conditions, le Verwaltungsgericht Wiesbaden (tribunal administratif de Wiesbaden) a décidé de surseoir à statuer et de poser à la Cour la question préjudicielle suivante :

« 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 2019/1157] 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]

c) à l'article 35, paragraphe 10, du RGPD

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

25. La demande de décision préjudicielle a été enregistrée au greffe de la Cour le 1er février 2022. Les gouvernements allemand, espagnol et polonais, le Parlement, le Conseil et la Commission européenne ainsi que le requérant au principal ont déposé des observations écrites. L'audience s'est tenue le 14 mars 2023.

IV. Appréciation

26. Par sa question, la juridiction de renvoi cherche à savoir si le règlement 2019/1157 est valide au regard du droit de l'Union. Elle demande, en particulier :

– premièrement, si l'article 21, paragraphe 2, TFUE constituait une base juridique appropriée pour l'adoption du règlement 2019/1157 et, en particulier, de son article 3, paragraphe 5, conformément à la procédure législative ordinaire qui y est visée ;

– deuxièmement, si l'article 3, paragraphe 5, du règlement 2019/1157 est compatible avec les articles 7 et 8 de la Charte, lus en combinaison avec l'article 52, paragraphe 1, de celle-ci, et

[11] Avis 7/2018 du Contrôleur européen de la protection des données, du 10 août 2018, sur la proposition de règlement relatif au renforcement de la sécurité des cartes d'identité des citoyens de l'Union et d'autres documents (JO 2018, C 338, p. 22) (ci-après l'« avis 7/2018 du CEPD »).

– troisièmement, si l'article 3, paragraphe 5, du règlement 2019/1157 est conforme à l'obligation de procéder à une analyse de l'impact relative à la protection des données au titre de l'article 35, paragraphe 10, du RGPD.

27. J'examinerai successivement chacun de ces différents motifs d'invalidité.

A. Base juridique pour l'adoption du règlement 2019/1157

28. Le premier motif d'invalidité concerne la base juridique pour l'adoption du règlement 2019/1157. En substance, la juridiction de renvoi nourrit des doutes quant à la question de savoir si ce règlement aurait dû être adopté sur le fondement de l'article 77, paragraphe 3, TFUE plutôt que sur celui de l'article 21, paragraphe 2, de ce traité. Au-delà du choix, d'un point de vue formel, de la base juridique appropriée du règlement 2019/1157, c'est la procédure législative applicable en vertu de l'une ou de l'autre disposition qui est en cause.

29. L'article 21 TFUE figure dans la deuxième partie du traité FUE, consacrée à la « non-discrimination et citoyenneté de l'Union ». Au paragraphe 1 de cet article, il est prévu que 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. Pour sa part, l'article 21, paragraphe 2, TFUE prévoit la possibilité pour l'Union d'adopter des dispositions visant à faciliter l'exercice de ce droit si une action apparaît nécessaire pour réaliser cet objectif et si les traités n'ont pas prévu des pouvoirs d'action à cet effet. Dans ce cas, la procédure législative ordinaire, qui implique la codécision du Parlement et du Conseil, s'applique.

30. En revanche, l'article 77, paragraphe 3, TFUE, qui concerne les « politiques relatives aux contrôles aux frontières, à l'asile et à l'immigration », figure au titre V de la troisième partie de ce traité, consacré à l'« Espace de liberté, de sécurité et de justice ». Il dispose que, si une action de l'Union apparaît nécessaire pour faciliter l'exercice du droit visé à l'article 20, paragraphe 2, sous a), TFUE – le droit de circuler et de séjourner librement sur le territoire des États membres –, le Conseil peut arrêter des dispositions concernant, entre autres, les passeports et les cartes d'identité. L'application de l'article 77, paragraphe 3, TFUE dépend également, d'après son libellé, de l'absence des pouvoirs d'action nécessaires prévus par les traités. Dans ce cas, une procédure législative spéciale s'applique, dans laquelle le Conseil statue à l'unanimité après consultation du Parlement.

31. Il ressort d'une jurisprudence constante de la Cour que le choix de la base juridique d'un acte de l'Union doit se fonder sur des éléments objectifs susceptibles de faire l'objet d'un contrôle juridictionnel, parmi lesquels figurent la finalité et le contenu de cet acte [12]. De plus, la Cour a établi que peut être pris en compte, pour déterminer la base juridique appropriée d'un acte de l'Union, le contexte juridique dans lequel s'inscrit une nouvelle réglementation, notamment en ce qu'un tel contexte est susceptible de fournir un éclairage sur le but de cette réglementation [13].

32. Quant à la présente affaire, je tiens à souligner, d'emblée, que la circonstance que, dans l'arrêt Schwarz, l'article 77, paragraphe 3, TFUE a été considéré comme la base juridique appropriée du règlement n° 2252/2004, qui établit l'obligation de recueil et de stockage d'empreintes digitales

[12] Arrêt du 3 décembre 2019, République tchèque/Parlement et Conseil (C-482/17, EU:C:2019:1035, point 31 et jurisprudence citée).

[13] Arrêt du 3 décembre 2019, République tchèque/Parlement et Conseil (C-482/17, EU:C:2019:1035, point 32 et jurisprudence citée).

pour les passeports des citoyens de l'Union [14], n'est pas, en soi, déterminante, contrairement à l'avis exprimé par la juridiction de renvoi, aux fins de déterminer si l'adoption du règlement 2019/1157 a été fondée à bon droit sur l'article 21, paragraphe 2, TFUE. En effet, la Cour a jugé de façon constante, conformément à la jurisprudence citée au point précédent des présentes conclusions, que c'est le but et le contenu de l'acte examiné qui doivent être pris en considération pour établir sa base juridique correcte, et non la base juridique d'autres actes de l'Union présentant le cas échéant des caractéristiques similaires [15].

33. S'agissant, d'une part, de l'objectif poursuivi par le règlement 2019/1157, je relève que l'article 1er de ce règlement, intitulé « Objet », prévoit que ledit règlement renforce les normes de sécurité applicables, notamment, aux cartes d'identité délivrées par les États membres à leurs ressortissants lorsqu'ils exercent leur droit à la libre circulation. Cette disposition constitue l'expression normative des considérants 1 à 5 du même règlement, lesquels, par référence au traité UE, au traité FUE, à l'article 45 de la Charte et à la directive 2004/38, évoquent l'objectif de faciliter l'exercice du droit des citoyens de l'Union à la libre circulation dans un environnement sûr [16].

34. En particulier, le considérant 4 du règlement 2019/1157 indique que la falsification de documents ou la description fallacieuse d'un fait matériel concernant les conditions liées au droit de séjour ont été identifiées comme des cas typiques de fraude liée à la libre circulation. En outre, il ressort du considérant 5 de ce règlement que la falsification de documents et la fraude résultent des différences considérables existant entre les niveaux de sécurité des cartes d'identité nationales délivrées par les États membres. Ces différences, selon ce même considérant, augmentent le risque de falsification et de fraude documentaire, et entraînent des difficultés pratiques pour les citoyens lorsqu'ils cherchent à exercer leur droit à la libre circulation. Enfin, le considérant 28 dudit règlement énonce que l'introduction de normes de sécurité renforcées devrait offrir des garanties suffisantes aux autorités publiques et aux entités privées pour leur permettre de se fier à l'authenticité des cartes d'identité lorsqu'elles sont utilisées par les citoyens de l'Union à des fins d'identification.

35. S'agissant, d'autre part, du contenu du règlement 2019/1157, l'obligation de recueillir et de stocker l'image d'empreintes digitales prévue par ce règlement, qui est en cause dans la présente affaire, fait partie d'un ensemble plus large de mesures applicables aux cartes nationales d'identité nouvellement délivrées, lesquelles sont, pour la plupart, énumérées à l'article 3 dudit règlement, sous l'intitulé « Normes de sécurité/format/spécifications ».

36. Lues à la lumière du considérant 17 du règlement 2019/1157, il apparaît que les mesures susmentionnées sont destinées à satisfaire les finalités de sécurité nécessaires à la vérification de l'authenticité d'un document et à l'établissement de l'identité d'une personne [17]. Le considérant 18 de ce règlement explique encore, à cet égard, que le stockage de données biométriques sur les cartes d'identité, à savoir une image faciale et deux empreintes digitales, représente une combinaison appropriée d'identification et d'authentification fiables avec un risque réduit de fraude, aux fins de renforcer la sécurité des cartes d'identité.

14 Arrêt Schwarz (point 20).

15 Voir, à cet égard, arrêt du 18 décembre 2014, Royaume-Uni/Conseil (C-81/13, EU:C:2014:2449, points 35 et 36 ainsi que jurisprudence citée).

16 Voir également considérant 46 du règlement 2019/1157.

17 Il est expressément indiqué dans ce considérant que l'établissement de normes minimales de sécurité et l'intégration de données biométriques dans les cartes d'identité sont des étapes importantes pour rendre leur utilisation dans l'Union plus sûre et pour permettre aux citoyens de l'Union de profiter pleinement de leurs droits à la libre circulation.

37. Il résulte de ce qui précède que le but du règlement 2019/1157 envisagé par le Parlement et le Conseil était essentiellement de faciliter le droit des citoyens de l'Union de se rendre et de séjourner dans tout État membre avec leur carte d'identité et de pouvoir présenter une telle carte comme preuve authentique et fiable de leur identité. Il s'agit également des termes employés par la Commission dans sa proposition de règlement [18], où est souligné, tout comme dans le règlement 2019/1157, la nécessité de réduire le risque de falsification et de fraude documentaire afin d'améliorer l'acceptation de ces cartes dans l'État membre autre que celui qui les délivre [19]. Cet objectif devait être atteint, compte tenu des dispositions figurant dans le règlement 2019/1157, en intégrant, dans les cartes nationales d'identité, des éléments communs de sécurité, qualifiés par ce même règlement de i) « normes minimales en matière de sécurité et de format » ainsi que de ii) « normes de sécurité renforcées » [20]. Cette dernière catégorie comprenait l'obligation de recueillir les empreintes digitales et de stocker une image de celles-ci sur un support hautement sécurisé.

38. Reste la question de savoir si, eu égard au but et au contenu du règlement 2019/1157, comme je l'ai déjà décrit, c'est à juste titre que le législateur de l'Union a considéré l'article 21, paragraphe 2, TFUE comme la base juridique appropriée pour l'adoption de ce règlement. Compte tenu du libellé de cette disposition, mentionnée au point 29 des présentes conclusions, cette question impliquerait que la Cour examine, premièrement, si ledit règlement peut être considéré comme ayant été adopté à bon droit en vue de faciliter l'exercice du droit de circuler et de séjourner librement sur le territoire des États membres ; deuxièmement, si une action de l'Union apparaissait nécessaire pour atteindre cet objectif et, troisièmement, si les traités ont prévu des pouvoirs d'action à cet effet.

1. Faciliter l'exercice du droit à la libre circulation

39. S'agissant, en premier lieu, de la question de savoir si le règlement 2019/1157 a été adopté à bon droit en vue de faciliter l'exercice du droit à la libre circulation, il importe de rappeler que, selon l'article 4 de la directive 2004/38, tout citoyen de l'Union a le droit de quitter le territoire d'un État membre en vue de se rendre dans un autre État membre (le droit de sortie). De même, selon l'article 5 de cette directive, les États membres doivent admettre les citoyens de l'Union sur leur territoire (le droit d'entrée). Ainsi que cela a été mis en évidence par ladite directive – et rappelé par le considérant 2 du règlement 2019/1157 –, les deux droits constituent l'essence même du droit à la libre circulation et, à ce titre, l'un des piliers de la citoyenneté de l'Union.

40. Toutefois, en vertu des dispositions susmentionnées, l'exercice du droit de sortie et d'entrée est subordonné à l'obligation de présenter une carte d'identité ou un passeport en cours de validité. Comme la Cour l'a indiqué dans sa jurisprudence, cette obligation vise à simplifier la solution des problèmes liés à la preuve du droit de séjour non seulement pour les citoyens de l'Union, mais aussi pour les autorités nationales [21]. Par conséquent, la confiance qu'ont les États membres dans le fait d'accueillir un citoyen de l'Union sur leurs territoires respectifs et, en fin de compte, l'exercice du droit de libre circulation par ce citoyen dépendent de la fiabilité de sa carte

[18] Voir, en ce sens, proposition de règlement du Parlement européen et du Conseil relatif au renforcement de la sécurité des cartes d'identité des citoyens de l'Union et des titres de séjour délivrés aux citoyens de l'Union et aux membres de leur famille exerçant leur droit à la libre circulation [COM(2018) 212 final], p. 4 (ci-après la « proposition de règlement de la Commission »).

[19] Pour le cadre conceptuel des objectifs généraux et spécifiques de la proposition de règlement de la Commission, voir le document de travail des services de la Commission – Analyse d'impact du 17 avril 2018 [SWD(2018) 110 final], p. 24 [en anglais] (ci-après l'« analyse d'impact de la Commission »].

[20] Voir considérant 28 du règlement 2019/1157.

[21] Arrêt du 17 février 2005, Oulane (C-215/03, EU:C:2005:95, point 22).

d'identité ou de son passeport en matière d'authenticité et d'identification [22]. Cela est d'autant plus vrai, ainsi qu'il résulte du considérant 4 du règlement 2019/1157, que la directive 2004/38 permet aux États membres de refuser, d'annuler ou de retirer tout droit conféré par cette directive en cas de fraude [23].

41. En outre, il importe de rappeler que l'exercice du droit à la libre circulation n'est pas limité aux contrôles aux frontières [24] ou à l'enregistrement administratif, comme le soutient à titre principal le requérant. Le droit à la libre circulation et au séjour permet aux citoyens de l'Union de s'immerger dans la vie quotidienne des autres résidents de l'État membre d'accueil. Les cartes nationales d'identité présentent ainsi les mêmes fonctions que pour ces résidents, ce qui implique que seule une preuve d'identité fiable et authentique, délivrée selon des normes de sécurité et des formats communs, facilite la pleine jouissance de la libre circulation. En l'absence de telles normes et de tels formats communs, et compte tenu de l'absence d'homogénéité des cartes nationales d'identité actuelles au sein de l'Union, comme je le relèverai ultérieurement [25], des obstacles et des difficultés peuvent surgir plus facilement, ce qui constitue l'enjeu principal décrit au considérant 5 du règlement 2019/1157.

42. L'utilisation des cartes nationales d'identité afin d'avoir accès aux services offerts par des entités publiques ou privées dans l'État membre d'accueil, en particulier lorsqu'une pièce d'identité est exigée par le droit national à de telles fins d'identification, est parlant à cet égard. Tel est le cas, par exemple, dans le cadre de l'accès à des services publics tels que la santé ou lorsqu'on traite avec des banques, des compagnies aériennes, des lieux de divertissement, des hôtels et d'autres établissements hôteliers, etc. De plus, l'utilisation de cartes nationales d'identité est essentielle pour bénéficier des droits étroitement liés au droit à la libre circulation et de séjour, tels que le droit de voter aux élections européennes et municipales et celui de s'y présenter en tant que candidat [26].

43. Dans ce contexte, je peine à soutenir, à la lumière du but et du contenu du règlement 2019/1157, que ce règlement n'a aucun rapport avec l'objectif de faciliter l'exercice du droit à la libre circulation. Au contraire, l'homogénéisation du format des cartes nationales d'identité et l'amélioration de leur fiabilité au moyen de normes de sécurité, y compris celles introduites par l'article 3, paragraphe 5, dudit règlement, ont une incidence directe sur l'exercice de ce droit, en augmentant la fiabilité de ces cartes – aussi bien du point de vue technique qu'en matière de perception du public, comme le relève à juste titre la Commission –, de sorte qu'elles seront, en tant que telles, plus facilement acceptées par les autorités des États membres et les entités fournissant des services [27]. En fin de compte, il s'agit d'une réduction des désagréments, des coûts et des obstacles administratifs pour les citoyens mobiles de l'Union.

22 Voir, également, article 8, paragraphe 3, de la directive 2004/38, intitulé « Formalités administratives à charge des citoyens de l'Union ».

23 Voir article 35 de la directive 2004/38.

24 Tel que c'est le cas, par exemple, des États membres comme l'Irlande, où les contrôles aux frontières intérieures restent en vigueur, ou concernant la réintroduction temporaire du contrôle aux frontières intérieures en vertu des articles 23 et suiv. du règlement (UE) 2016/399 du Parlement européen et du Conseil, du 9 mars 2016, concernant un code de l'Union relatif au régime de franchissement des frontières par les personnes (code frontières Schengen) (JO 2016, L 77, p. 1), tel que modifié.

25 Voir point 47 des présentes conclusions.

26 Les avantages pour les droits démocratiques européens et pour l'initiative citoyenne sont également mentionnés dans l'analyse d'impact de la Commission (point 6.1).

27 Voir, en ce sens, considérant 15, dernière phrase, du règlement 2019/1157, ainsi que le considérant 28 de ce règlement, qui, comme il a déjà été indiqué, précise que ces deux types de mesures aident les États membres, d'une part, à s'appuyer sur l'authenticité de ces documents et, d'autre part, à offrir des garanties suffisantes aux autorités publiques et aux entités privées pour leur permettre de se fier à ces documents lorsqu'ils sont utilisés par les citoyens de l'Union à des fins d'identification.

44. J'ajouterai brièvement que, même si les passeports, qui sont déjà soumis à l'obligation de recueillir et de stocker les empreintes digitales au titre du règlement n° 2252/2004, sont des documents qui peuvent par ailleurs être utilisés pour l'exercice du droit à la libre circulation par les citoyens de l'Union, cela n'exclut pas que les cartes nationales d'identité répondent à cette même finalité en vertu de la directive 2004/38 [28] et que, du point de vue du législateur de l'Union, ces cartes pouvaient nécessiter des formats plus harmonisés et des normes de sécurité plus solides afin de les rendre plus fiables et, partant, plus facilement admissibles.

45. La première condition énoncée à l'article 21, paragraphe 2, TFUE, à savoir l'exigence que le règlement 2019/1157 a été adopté à bon droit en vue de faciliter l'exercice du droit de circuler et de séjourner librement sur le territoire des États membres, est donc, à mon sens, remplie.

2. Sur la question de savoir si une action apparaît nécessaire

46. S'agissant, en deuxième lieu, de la question de savoir si une action de l'Union était nécessaire pour atteindre l'objectif consistant à faciliter l'exercice du droit à la libre circulation, je dois souligner qu'il ne s'agit pas d'un élément qui a été spécifiquement soulevé par la juridiction de renvoi ou qui a été remis en cause par le requérant au principal. En tout état de cause, j'attirerai l'attention de la Cour sur l'analyse d'impact effectuée par la Commission, qui accompagne la proposition de règlement de cette institution [29].

47. Dans cette analyse, la Commission explique que les citoyens européens sont de plus en plus mobiles – à l'intérieur et à l'extérieur de l'Union –, ce qui constitue, sans aucun doute, une réalisation majeure de l'intégration européenne [30]. À cet égard, la Commission souligne que, alors que la directive 2004/38 a fixé les conditions d'exercice du droit de circuler et de séjourner librement, cette directive ne régissait pas le format et les normes de sécurité des cartes d'identité nationales, raison pour laquelle plus de 250 versions valides de ces cartes sont en cours de circulation dans l'Union [31]. Dans ces conditions, l'analyse d'impact de la Commission identifie, en tant que problèmes pour l'exercice du droit à la libre circulation, une acceptation insuffisante des cartes nationales d'identité par les États membres, une augmentation des niveaux de fraude documentaire ainsi que l'absence d'authentification par rapport à ces cartes et la complexité de leur émission et de leur administration [32]. Dans son analyse, la Commission conclut que, s'il devient de plus en plus nécessaire d'utiliser les cartes nationales d'identité, des difficultés considérables pour l'exercice des droits de libre circulation subsisteraient ou augmenteraient en l'absence d'une action appropriée [33].

48. À mon avis, les questions précédentes, qui sont davantage développées dans l'analyse d'impact de la Commission, montrent l'utilisation croissante des droits de libre circulation par les citoyens de l'Union, ce qui constitue un fait notoire. Dans le même temps, ces questions mettent en évidence les difficultés et les risques actuels qui se manifestent dans l'exercice de ces droits en raison de l'absence d'homogénéité en ce qui concerne les formats et les éléments de sécurité des cartes nationales d'identité. Compte tenu du large pouvoir d'appréciation reconnu au législateur

[28] Voir, en ce sens, arrêt du 16 avril 2015, Willems e.a. (C-446/12 à C-449/12, EU:C:2015:238, point 39).

[29] Voir note en bas de page 19 des présentes conclusions.

[30] Voir analyse d'impact de la Commission (point 1.1), qui indique que plus de 15 millions de citoyens de l'Union résident dans un autre État membre et que plus de 11 millions de citoyens travaillent dans un autre État membre, en plus des nombreux étudiants qui se déplacent dans l'Union à des fins d'éducation et de formation.

[31] Analyse d'impact de la Commission (point 1.2 et annexe 5).

[32] Analyse d'impact de la Commission (point 2.1 et figure 2.1).

[33] Analyse d'impact de la Commission (point 2.2).

de l'Union lorsqu'il est appelé à effectuer des appréciations complexes [34], il ne saurait y avoir de doute quant à l'absence d'erreur du Parlement et du Conseil lorsqu'ils ont envisagé qu'une action de l'Union serait nécessaire pour atteindre l'objectif de faciliter l'exercice de la libre circulation.

49. La deuxième condition énoncée à l'article 21, paragraphe 2, TFUE est donc, selon moi, également remplie.

3. Pouvoirs d'action prévus à cet effet

50. En troisième lieu, l'adoption d'un acte de l'Union sur le fondement de l'article 21, paragraphe 2, TFUE est subordonnée à la condition que « les traités [n'ont pas] prévu des pouvoirs d'action à cet effet ». Dans l'ordonnance de renvoi, la juridiction de renvoi considère que l'article 77, paragraphe 3, TFUE constitue une base juridique plus spécifique pour l'intégration de nouveaux éléments de sécurité aux cartes nationales d'identité des États membres. Pour cette raison, elle a estimé que l'article 77, paragraphe 3, TFUE aurait dû être utilisé en tant que base juridique au lieu de l'article 21, paragraphe 2, TFUE lors de l'adoption du règlement 2019/1157.

51. À titre liminaire, je tiens à rappeler que, selon une jurisprudence constante, le cumul de deux bases juridiques est exclu lorsque les procédures prévues par l'une ou l'autre des bases juridiques sont incompatibles [35]. En l'espèce, les procédures législatives applicables au titre de l'article 21, paragraphe 2, TFUE, d'une part, et de l'article 77, paragraphe 3, TFUE, d'autre part, s'excluent mutuellement, ce qui implique que le recours à la première de ces dispositions pour adopter le règlement 2019/1157 ne pourrait être validé si la Cour devait conclure que l'article 77, paragraphe 3, TFUE aurait dû constituer la base juridique appropriée pour l'adoption de ce règlement.

52. En tout état de cause, compte tenu du libellé et de la systématique de l'article 77, paragraphe 3, TFUE, ainsi que de l'économie du même traité, je ne pense pas qu'il y ait lieu de confirmer la thèse de la juridiction de renvoi.

53. Premièrement, ainsi qu'il a été indiqué au point 30 des présentes conclusions, l'article 77, paragraphe 3, TFUE figure dans le titre V de la troisième partie du traité FUE, consacré à l'« Espace de liberté, de sécurité et de justice », notamment au chapitre 2 de celui-ci, qui concerne les « [p]olitiques relatives aux contrôles aux frontières, à l'asile et à l'immigration ». Cette disposition se trouve après l'article 77, paragraphe 1, TFUE, qui prévoit que l'Union développe une politique visant à atteindre certains objectifs en ce qui concerne, en substance, les contrôles aux frontières. Il se trouve également après l'article 77, paragraphe 2, TFUE, qui permet au Parlement et au Conseil d'adopter, au moyen de la procédure législative ordinaire, des mesures concernant cette même politique.

54. Le contenu et la systématique de l'article 77 TFUE invitent ainsi à considérer que, même si son paragraphe 3 confère au Conseil la compétence pour adopter des dispositions relatives aux passeports et aux cartes d'identité, aux fins de faciliter l'exercice du droit de circuler et de séjourner librement, cette compétence doit être comprise comme se référant au contexte de la politique de contrôle aux frontières. Une mesure de l'Union allant au-delà de ce contenu spécifique, nonobstant les exigences de la procédure législative applicable, ne relèverait pas du champ d'application de l'article 77, paragraphe 3, TFUE.

[34] Voir, entre autres, arrêt du 22 juin 2017, E.ON Biofor Sverige (C-549/15, EU:C:2017:490, point 50 et jurisprudence citée).

[35] Voir, notamment, arrêt du 11 juin 2014, Commission/Conseil (C-377/12, EU:C:2014:1903, point 34).

55. En l'occurrence, l'introduction de normes, de formats et de spécifications uniformes concernant la sécurité des cartes nationales d'identité, y compris ceux définis à l'article 3, paragraphe 5, du règlement 2019/1157, est certainement susceptible d'avoir une incidence sur les contrôles aux frontières [36]. Or, ainsi que je l'ai fait valoir dans les présentes conclusions, ce règlement couvre une partie plus large de la vie des citoyens de l'Union, ce qui exclut qu'il soit cantonné au seul domaine des contrôles aux frontières. À cet égard, il pourrait être utile de rappeler que, si l'examen d'un acte de l'Union démontre que celui-ci poursuit plusieurs finalités et si l'une de ces finalités est identifiable comme étant principale ou prépondérante, tandis que les autres ne sont qu'accessoires, cet acte doit alors être fondé sur une seule base juridique, à savoir celle correspondant à cette finalité [37]. Quant audit règlement, il me semble évident qu'il affecte le droit de circuler et de séjourner librement à de nombreux égards, tout en n'ayant qu'un impact partiel sur les contrôles aux frontières.

56. Deuxièmement, il importe de relever que, selon l'article 77, paragraphe 3, TFUE, cette disposition n'est applicable que si les pouvoirs d'action nécessaires pour atteindre son objectif ne sont pas prévus par d'autres dispositions des traités, ce qui constitue une clause subsidiaire rédigée dans des termes analogues à ceux de l'article 21, paragraphe 2, TFUE. La question qui se pose est celle de savoir si c'est l'article 21, paragraphe 2, TFUE ou l'article 77, paragraphe 3, TFUE qui constitue une disposition plus spécifique par rapport à l'autre, en ce qui concerne, notamment, le droit de circuler et de séjourner librement sur le territoire des États membres.

57. À cet égard, je souhaiterais souligner, d'une part, que l'article 77, paragraphe 3, TFUE se réfère expressément à l'article 20 du même traité, qui institue la citoyenneté de l'Union et, plus particulièrement, à son paragraphe 2, sous a), qui prévoit que cette citoyenneté englobe le droit de circuler et de séjourner librement sur le territoire des États membres. L'article 77, paragraphe 3, TFUE dispose ensuite que le Conseil est compétent pour arrêter des dispositions concernant, entre autres, les cartes d'identité pour faciliter le droit visé à l'article 20, paragraphe 2, sous a), TFUE, si les traités n'ont pas prévu de pouvoirs d'action à cet effet. Comme je l'ai déjà relevé, l'article 21 TFUE précise à son tour le contenu de l'article 20, paragraphe 2, sous a), TFUE en prévoyant, notamment, que le droit qui y figure est soumis aux limitations et conditions prévues par les traités et par les dispositions prises pour leur application, précisément au moyen du paragraphe 2 de celui-ci. Dans ce contexte, je serais donc encline à considérer que, s'agissant de l'article 20, paragraphe 2, TFUE, l'article 21 du même traité constitue une disposition plus spécifique, ce qui a pour effet de rendre inapplicable la clause subsidiaire de l'article 77, paragraphe 3, TFUE et, donc, la procédure législative spéciale prévue à cette disposition.

58. D'autre part, ainsi que le fait valoir la Commission, le champ d'application de la clause subsidiaire résultant de l'article 21, paragraphe 2, TFUE, qui permet l'adoption de dispositions destinées à faciliter la libre circulation des personnes, sauf si les traités ont prévu des pouvoirs d'action à cet effet, semble circonscrit aux articles du traité FUE figurant au titre IV de la troisième partie de celui-ci, à savoir son article 45, relatif à la libre circulation des travailleurs, et

[36] Ainsi que le relève le gouvernement espagnol, l'adoption du règlement 2019/1157 s'inscrivait dans l'objectif d'améliorer la sécurité des documents de voyage, notamment à la suite de la modification du code frontières Schengen, qui a introduit l'obligation de contrôler systématiquement toutes les personnes et de vérifier leurs documents de voyage – indépendamment de la nationalité du titulaire – dans le système d'information Schengen (SIS) et dans la base de données d'Interpol sur les documents de voyage volés ou perdus (SLTD). Voir, en ce sens, règlement (UE) 2017/458 du Parlement européen et du Conseil, du 15 mars 2017, modifiant le règlement 2016/399 en ce qui concerne le renforcement des vérifications dans les bases de données pertinentes aux frontières extérieures (JO 2017, L 74, p. 1). Voir également l'analyse d'impact de la Commission, point 1.2 (p. 5).

[37] Voir, notamment, arrêt du 20 novembre 2018, Commission/Conseil (AMP Antarctique) (C-626/15 et C-659/16, EU:C:2018:925, point 77 et jurisprudence citée).

ses articles 49 et 56, relatifs au droit d'établissement et à la libre prestation de services sur le territoire d'un autre État membre. C'est ce qui ressort d'un point de vue systématique, en raison du risque que les dispositions du traité concernant, d'une part, le droit des citoyens de l'Union de se déplacer et de séjourner librement au sein de l'Union et, d'autre part, les droits à la libre circulation en tant qu'éléments essentiels du marché intérieur se recoupent. La jurisprudence de la Cour corrobore effectivement cette lecture [38] dans la mesure où, selon cette jurisprudence, l'article 21 TFUE trouve une expression spécifique dans les dispositions assurant la libre circulation, laissant entendre, en outre, que si une affaire relève du champ d'application de l'une de ces dispositions, l'article 21 TFUE renonce à sa position en tant que base juridique appropriée pour l'adoption de dispositions destinées à faciliter le droit de circuler et de séjourner librement [39].

59. Enfin, je relèverai brièvement que la circonstance que l'article 77, paragraphe 3, TFUE se réfère spécifiquement aux cartes d'identité dans son libellé, comme le souligne la juridiction de renvoi, n'est pas déterminante pour que cette disposition soit considérée comme une disposition plus spécifique par rapport à l'article 21, paragraphe 2, TFUE. En effet, l'article 77, paragraphe 3, TFUE vise également, par exemple, les titres de séjour, dont le modèle uniforme, notamment pour les ressortissants de pays tiers, a été établi par le règlement (CE) n° 1030/2002 [40], y compris les éléments de sécurité minimale et l'obligation de stockage des données biométriques. Or, ce règlement et ses modifications ont été adoptés au moyen de la procédure législative ordinaire sur le fondement de l'article 63, point 3, TCE, devenu par la suite l'article 79 TFUE, et non pas sur le fondement de la disposition antérieure à l'article 77, paragraphe 3, TFUE. La raison en est que les permis de séjour sont des documents destinés à être utilisés en interne dans l'État membre de délivrance et non aux fins de contrôle aux frontières, comme c'est le cas également, dans la majorité des cas, des cartes nationales d'identité.

60. Il s'ensuit que l'article 77, paragraphe 3, TFUE ne constitue pas une disposition plus spécifique aux fins de faciliter l'exercice du droit de circuler et de séjourner librement sur le territoire des États membres par rapport à l'article 21, paragraphe 2, TFUE et, par conséquent, que la troisième condition énoncée à cette dernière disposition est remplie.

61. Eu égard à ce qui précède, et comme l'analyse que je propose révèle que les trois conditions qui ressortent du libellé de l'article 21, paragraphe 2, TFUE sont remplies, je conclurais que, en utilisant cette disposition comme base juridique du règlement 2019/1157, le Parlement et le Conseil ont adopté ce règlement de manière adéquate.

62. Le premier motif soulevé par la juridiction de renvoi ne devrait pas conduire la Cour à déclarer l'invalidité du règlement 2019/1157 et, en particulier, de son article 3, paragraphe 5.

B. Les articles 7 et 8 de la Charte

63. Le deuxième motif d'invalidité évoqué dans la demande de décision préjudicielle porte sur le point de savoir si l'obligation de recueillir et de stocker une image de deux empreintes digitales dans les cartes d'identité nouvellement délivrées par les États membres, prévue à l'article 3, paragraphe 5, du règlement 2019/1157, constitue une limitation injustifiée des articles 7 et 8 de la Charte, lus en combinaison avec l'article 52, paragraphe 1, de celle-ci.

[38] Voir, en ce sens, arrêt du 20 mai 2010, Zanotti (C-56/09, EU:C:2010:288).

[39] Voir arrêt du 20 mai 2010, Zanotti (C-56/09, EU:C:2010:288, point 24 et jurisprudence citée).

[40] Voir article 4 ter du règlement du Conseil du 13 juin 2002 établissant un modèle uniforme de titre de séjour pour les ressortissants de pays tiers (JO 2002, L 157, p. 1).

1. Limitation

64. L'article 7 de la Charte prévoit que toute personne a droit au respect de sa vie privée et familiale, de son domicile et de ses communications. Selon l'article 8, paragraphe 1, de celle-ci, toute personne a droit à la protection des données à caractère personnel la concernant. Même si ces deux dispositions sont consacrées à deux droits fondamentaux différents, la Cour les a traditionnellement appliquées conjointement lorsqu'elle examine, comme en l'espèce, la conformité avec la Charte des dispositions européennes ou nationales relatives au traitement de données à caractère personnel [41].

65. La Cour a également déclaré que le respect du droit à la vie privée à l'égard du traitement des données à caractère personnel, reconnu par les articles 7 et 8 de la Charte, se rapporte à toute information concernant une personne physique identifiée ou identifiable [42]. Tel est manifestement le cas des identifiants biométriques et, en particulier, des empreintes digitales en cause dans le règlement 2019/1157, qui contiennent des informations uniques sur des personnes physiques et permettent leur identification précise [43].

66. Par ailleurs, dans l'arrêt Schwarz, la Cour a jugé que l'intégration obligatoire des empreintes digitales dans les passeports nouvellement délivrés par les États membres, comme le prévoit le règlement n° 2252/2004, devait être considérée comme un traitement de données à caractère personnel et que cette intégration constituait une limitation des droits garantis par les articles 7 et 8 de la Charte [44]. Conformément au point de vue défendu par l'ensemble des parties dans la présente procédure, cet arrêt conduit à considérer que le règlement 2019/1157, qui introduit des mesures similaires concernant les cartes nationales d'identité, établit une limitation des deux droits fondamentaux protégés par ces articles.

67. Plus précisément, cette limitation devrait être définie par référence aux deux mesures prévues à l'article 3, paragraphe 5, du règlement 2019/1157, à savoir, d'une part, le recueil en tant que tel des empreintes digitales, dont la procédure est précisée à l'article 10, paragraphe 1, de ce règlement, et, d'autre part, l'intégration définitive de ces empreintes digitales sur un support de stockage hautement sécurisé dans chaque carte d'identité nouvellement délivrée par les États membres [45].

68. En outre, comme l'indique le Parlement, il convient de tenir compte de la mesure prévue à l'article 10, paragraphe 3, du règlement 2019/1157. En substance, cette disposition prévoit que les éléments d'identification biométriques stockés aux fins de la personnalisation des cartes d'identité doivent être conservés par les autorités publiques jusqu'à la date de remise de la carte d'identité à son titulaire et, en tout état de cause, pas plus de 90 jours à compter de la date de délivrance. Le fait de stocker ces éléments d'identification de cette manière accroît le risque d'un accès indu des

41 Voir arrêt Schwarz (point 25), et arrêt du 8 avril 2014, Digital Rights Ireland e.a. (C-293/12 et C-594/12, EU:C:2014:238, point 29). À comparer avec les conclusions de l'avocat général Cruz Villalón dans les affaires jointes Digital Rights Ireland e.a. (C-293/12 et C-594/12, EU:C:2013:845, point 64), où celui-ci fait valoir que, dans le cas de données qui ne concernent pas la vie privée, seul l'article 8 de la Charte devrait s'appliquer.

42 Arrêt du 3 octobre 2019, A e.a. (C-70/18, EU:C:2019:823, point 54 et jurisprudence citée).

43 Arrêt du 3 octobre 2019, A e.a. (C-70/18, EU:C:2019:823, point 55 et jurisprudence citée). Voir également l'analyse d'impact de la Commission (point 6.1, p. 34 et 35), qui souligne que les données biométriques doivent être cryptées et que, à cette fin, des clés cryptographiques doivent être échangées avec les services spécifiques, à savoir les gardes-frontières et les services de police.

44 Arrêt Schwarz (points 24 à 30).

45 Ce recueil doit être effectué conformément aux spécifications techniques établies par la décision C(2018) 7767 de la Commission, citée à la note en bas de page 9 des présentes conclusions.

autorités publiques aux éléments d'identification biométriques recueillis en vertu de l'article 3, paragraphe 5, du règlement 2019/1157 et ne devrait donc pas être ignoré lors de l'examen de la limitation, introduite par cette disposition, des droits garantis par les articles 7 et 8 de la Charte.

69. Enfin, l'article 11 du règlement 2019/1157, intitulé « Protection des données à caractère personnel et responsabilité », prévoit, notamment à son paragraphe 6, la possibilité pour les autorités nationales compétentes et les agences de l'Union d'utiliser les cartes nationales d'identité sur lesquelles sont stockées des empreintes digitales aux fins de la vérification de l'authenticité de la carte et de l'identité du titulaire. À nouveau, c'est dans le cadre de cette utilisation qu'une menace pourrait survenir en ce qui concerne les éléments d'identification biométriques recueillis conformément à l'article 3, paragraphe 5, du règlement 2019/1157.

70. Il résulte de ce qui précède que, afin de définir la limitation des droits garantis par les articles 7 et 8 de la Charte, introduite dans la présente affaire, et de vérifier si cette limitation peut être justifiée, l'examen de la Cour devrait être effectué non seulement au regard du recueil d'empreintes digitales et de leur intégration dans les cartes nationales d'identité nouvellement délivrées par les États membres, mais également des deux mesures supplémentaires qui, en raison de leur lien étroit avec les éléments d'identification biométriques visés à l'article 3, paragraphe 5, du règlement 2019/1157 en matière de stockage et d'utilisation ultérieure, ne devraient pas être isolées lors de cet examen.

2. Justification de la limitation

71. En ce qui concerne la question de savoir si la limitation résultant du règlement 2019/1157, telle que décrite précédemment, peut être justifiée, il convient de relever d'emblée que l'article 8, paragraphe 2, de la Charte permet le traitement de données à caractère personnel si la personne concernée y consent ou lorsqu'un autre fondement légitime prévu par la loi s'applique. En l'espèce, il est évident que les citoyens d'un État membre qui demandent la délivrance d'une carte d'identité nationale ne peuvent pas s'opposer, en raison du caractère obligatoire des mesures prévues à l'article 3, paragraphe 5, du règlement 2019/1157, au traitement de leurs empreintes digitales [46]. Par conséquent, il convient de vérifier si ce traitement peut être justifié en vertu d'une autre base juridique légitime.

72. Selon une jurisprudence constante de la Cour, les droits reconnus par les articles 7 et 8 de la Charte n'apparaissent pas comme des prérogatives absolues, mais doivent être pris en considération par rapport à leur fonction dans la société [47]. À cet égard, l'article 52, paragraphe 1, première phrase, de la Charte prévoit que toute limitation de l'exercice des droits et libertés reconnus par celle-ci doit être prévue par la loi et respecter le contenu essentiel de ces droits et libertés. L'article 52, paragraphe 1, seconde phrase, de la Charte prévoit en outre que, dans le respect du principe de proportionnalité, des limitations ne peuvent être apportées à ces droits et libertés 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 des libertés d'autrui [48].

[46] Voir, en ce qui concerne le caractère obligatoire des cartes nationales d'identité en République fédérale d'Allemagne, article 1^er, paragraphe 1, du PAuswG, tel qu'exposé au point 14 des présentes conclusions.

[47] Arrêt Schwarz (point 33 et jurisprudence citée).

[48] Arrêt Schwarz (point 34). Voir également arrêt du 8 avril 2014, Digital Rights Ireland e.a. (C-293/12 et C-594/12, EU:C:2014:238, point 38).

73. En l'occurrence, ainsi que le concède la juridiction de renvoi, aucune question ne se pose en ce qui concerne les exigences posées par l'article 52, paragraphe 1, première phrase, de la Charte. En effet, les limitations aux articles 7 et 8 de celle-ci découlant du règlement 2019/1157 sont prévues par la loi sous la forme d'un règlement, qui, dans le cas de la République fédérale d'Allemagne, a même été transposé en droit national [49]. En outre, compte tenu des différentes garanties offertes par l'article 3, paragraphe 5, l'article 10, paragraphes 1 et 3, et l'article 11, paragraphe 6, du règlement 2019/1157, en particulier en ce qui concerne le recueil, le stockage et l'utilisation d'empreintes digitales dans les cartes nationales d'identité nouvellement délivrées, comme je le décrirai plus loin [50], l'essence des droits consacrés par ces deux dispositions est respectée.

74. La question demeure de savoir si ces limitations sont conformes au principe de proportionnalité et, en particulier, si elles sont nécessaires et répondent effectivement à des objectifs d'intérêt général reconnus par l'Union, conformément à l'article 52, paragraphe 1, seconde phrase, de la Charte.

75. S'agissant de la question de savoir si les limitations résultant du règlement 2019/1157 répondent à un objectif d'intérêt général, j'ai déjà expliqué, dans le cadre de mon analyse du premier motif d'invalidité [51], que ce règlement vise à faciliter le droit à la libre circulation des citoyens de l'Union en rendant les cartes nationales d'identité plus fiables en matière d'authenticité et d'identification. En substance, il ressort de l'article 1er de ce règlement, lu à la lumière, notamment, des considérants 4, 5, 18 et 28 dudit règlement, que l'absence d'homogénéité en ce qui concerne les formats et les éléments de sécurité des cartes nationales d'identité accroît le risque de falsification et de fraude documentaire, dont la prévention constitue ainsi l'un des objectifs du même règlement en vue de favoriser l'acceptation de ces cartes dans les États membres autres que celui d'émission.

76. J'estime donc que, dans la mesure où le recueil et le stockage d'empreintes digitales dans les cartes nationales d'identité nouvellement délivrées, comme prévu à l'article 3, paragraphe 5, du règlement 2019/1157, visent à éviter que ces cartes deviennent la cible de falsifications et d'utilisations frauduleuses par des personnes autres que leur titulaire réel – en facilitant ainsi l'exercice du droit à la libre circulation tel que consacré, notamment, à l'article 45 de la Charte –, les limitations introduites par le règlement 2019/1157 poursuivent un objectif d'intérêt général au sens de l'article 52, paragraphe 1, de la Charte [52]. Une interprétation similaire a été retenue par la Cour dans l'arrêt Schwarz [53], qui est, à mon avis, analogue à la présente affaire.

77. En ce qui concerne la proportionnalité des limitations apportées par le règlement 2019/1157, il ressort d'une jurisprudence constante de la Cour que le principe de proportionnalité exige que les actes des institutions de l'Union soient aptes à réaliser les objectifs légitimes poursuivis par la réglementation en cause et ne dépassent pas les limites de ce qui est approprié et nécessaire à la réalisation de ces objectifs [54].

[49] Voir article 5, paragraphe 9, du PAuswG, tel qu'exposé au point 15 des présentes conclusions.

[50] Voir points 97 à 107 des présentes conclusions.

[51] Voir points 33 à 37 des présentes conclusions.

[52] Voir également l'analyse d'impact de la Commission (point 6.1, p. 34), qui indique en outre que l'exercice des droits politiques fondamentaux (articles 39 et 40 de la Charte) ainsi que l'exercice du droit de pétition (article 44 de la Charte) seront positivement affectés par le renforcement des éléments de sécurité des cartes nationales d'identité.

[53] Arrêt Schwarz (point 36).

[54] Voir arrêt du 8 avril 2014, Digital Rights Ireland e.a. (C-293/12 et C-594/12, EU:C:2014:238, point 46 et jurisprudence citée).

78. En outre, dès lors que des ingérences dans des droits fondamentaux sont en cause, l'étendue du pouvoir d'appréciation du législateur de l'Union peut s'avérer limitée en fonction d'un certain nombre d'éléments, parmi lesquels figurent, notamment, le domaine concerné, la nature du droit en cause garanti par la Charte, la nature et la gravité de l'ingérence ainsi que la finalité de celle-ci [55].

79. En l'occurrence, il est vrai que le recueil d'empreintes digitales et leur stockage dans les cartes nationales d'identité nouvellement délivrées ne constituent pas, en eux-mêmes, des mesures particulièrement intenses quant à la limitation qu'elles apportent aux droits garantis par les articles 7 et 8 de la Charte. En effet, d'une part, le recueil d'empreintes digitales n'est pas une opération revêtant un caractère intime [56] et, d'autre part, les éléments d'identification biométriques stockés dans une carte nouvellement délivrée restent, en vertu du règlement 2019/1157, à la seule disposition du titulaire de la carte.

80. Toutefois, la limitation introduite par le règlement 2019/1157 concerne la protection des données à caractère personnel, qui, selon la jurisprudence de la Cour, joue un rôle important au regard du droit fondamental au respect de la vie privée [57]. En outre, les mesures qui accompagnent le recueil et le stockage d'empreintes digitales, telles que je les ai décrites aux points 68 et 69 des présentes conclusions, sont de nature à accroître le risque d'un accès indu des autorités publiques aux éléments d'identification biométriques et d'abus à cet égard. Enfin, comme le relève la juridiction de renvoi, il convient de tenir compte de l'incidence considérable du règlement 2019/1157 sur la population de l'Union, dont l'obligation d'inclure une image des empreintes digitales dans les cartes d'identité nouvellement délivrées touche potentiellement 85 % des citoyens de l'Union, compte tenu du caractère obligatoire de ces cartes dans la majorité des États membres [58].

81. Pour toutes ces raisons, le pouvoir d'appréciation du législateur de l'Union devrait être considéré, selon moi, comme réduit, de sorte que le contrôle de ce pouvoir devrait être strict. Cela étant, j'estime que les limitations découlant du règlement 2019/1157 et, en particulier, de l'article 3, paragraphe 5, de celui-ci, sont appropriées, nécessaires et ne vont pas au-delà de ce qui est indispensable pour atteindre l'objectif principal de ce règlement.

82. En premier lieu, s'agissant de la question de savoir si le recueil et le stockage d'empreintes digitales dans les cartes nationales d'identité nouvellement délivrées sont aptes à atteindre l'objectif poursuivi par le règlement 2019/1157, il est constant – et la Cour l'a d'ailleurs jugé dans l'arrêt Schwarz [59] – que la conservation des empreintes digitales sur un support de stockage hautement sécurisé est susceptible de réduire le risque de falsification des documents nationaux, compte tenu du caractère unique des empreintes digitales à des fins d'identification et de la sophistication technique appliquée à cette conservation [60]. En réduisant le risque de falsification des cartes nationales d'identité, l'acceptation de ces cartes dans les États membres autres que celui de leur délivrance sera accrue, ce qui facilitera, en fin de compte, l'exercice du droit à la

[55] Voir arrêt du 8 avril 2014, Digital Rights Ireland e.a. (C-293/12 et C-594/12, EU:C:2014:238, point 47). Voir également, en ce qui concerne l'article 8 de la CEDH, arrêt de la Cour EDH du 4 décembre 2008, S. et Marper c. Royaume-Uni (CE:ECHR:2008:1204JUD003056204, § 102).

[56] Arrêt *Schwarz* (point 48).

[57] Arrêt Schwarz (point 48).

[58] Voir avis 7/2018 du CEPD (p. 3).

[59] Voir, en ce sens, arrêt Schwarz (point 41).

[60] Deux individus ne peuvent pas avoir les mêmes empreintes digitales, pas même les vrais jumeaux. De plus, ces empreintes digitales ne changent pas, même avec le temps, à moins que la couche profonde ou « basale » de la peau ne soit détruite ou volontairement modifiée par chirurgie plastique. Il existe trois grandes classes de formes des dessins digitaux : les arcs, les boucles et les verticilles. La forme, la taille, le nombre et la disposition des détails qui caractérisent ces motifs rendent chaque empreinte digitale unique. Voir, en ce sens, https://www.interpol.int/fr/Notre-action/Police-scientifique/Empreintes-digitales.

libre circulation des citoyens de l'Union [61]. Dans cette perspective, je ne crois pas qu'un doute doive subsister quant au caractère approprié de l'utilisation d'empreintes digitales pour atteindre l'objectif du règlement 2019/1157 [62].

83. La juridiction de renvoi souligne toutefois que le recueil et le stockage d'empreintes digitales permettent uniquement de vérifier si les données biométriques intégrées dans une carte nationale d'identité correspondent aux données biométriques de son titulaire, mais ne permet pas nécessairement l'identification de cette personne. Selon elle, une telle identification ne peut être effectuée qu'en comparant, d'une part, les données biométriques stockées sur la carte d'identité avec, d'autre part, les données biométriques stockées dans une base de données absolument infalsifiable. Dans cette perspective, la juridiction de renvoi se demande si l'intégration obligatoire des empreintes digitales dans les cartes nationales d'identité peut répondre à l'objectif du règlement 2019/1157.

84. À cet égard, je soulignerais que l'argumentation de la juridiction de renvoi n'est pas de nature à remettre en cause le fait que l'intégration d'empreintes digitales dans les cartes nationales d'identité est en soi un moyen efficace d'améliorer le niveau d'authenticité et de fiabilité de ces cartes et, partant, leur acceptation dans le cadre de l'exercice du droit à la libre circulation. Cette argumentation repose uniquement sur la prémisse selon laquelle l'intégration d'empreintes digitales dans les cartes nationales d'identité pourrait ne pas être totalement fiable, dès lors qu'elles peuvent encore être falsifiées, ce qui signifie que l'objectif poursuivi par le règlement 2019/1157 pourrait ne pas être pleinement atteint.

85. L'existence d'une infalsifiabilité absolue des cartes nationales d'identité après l'adoption du règlement 2019/1157, y compris des mesures imposées par l'article 3, paragraphe 5, de ce règlement, est une question qui ne saurait être appréciée à la lumière des éléments dont dispose la Cour. Cela étant, il découle de l'arrêt Schwarz que la circonstance qu'une méthode de lutte contre la falsification et l'utilisation frauduleuse n'est pas totalement fiable n'est pas déterminante pour qu'elle puisse être considérée comme inappropriée aux fins de l'interprétation de l'article 52, paragraphe 1, de la Charte. En effet, il suffit que la méthode réduise considérablement le risque de falsification qui existerait si cette même méthode n'était pas utilisée [63].

86. Par conséquent, même si le recueil et le stockage d'empreintes digitales dans les cartes d'identité nouvellement délivrées ne peuvent être considérés comme une mesure garantissant de manière absolue leur caractère infalsifiable, cela ne remet pas en cause leur aptitude à empêcher la falsification et la fraude documentaire et, partant, à faciliter le droit à la libre circulation des citoyens de l'Union. Le fait, également relevé par la juridiction de renvoi, que le recueil et l'intégration des empreintes digitales ne s'appliquent qu'aux cartes d'identité nouvellement délivrées et que les anciennes cartes restent temporairement valides ne remet pas non plus en

[61] Voir, à cet égard, considérant 28 du règlement 2019/1157, mentionné à la note en bas de page 27 des présentes conclusions.

[62] Comme je l'ai déjà indiqué dans les présentes conclusions, le droit de l'Union établit déjà, à des fins similaires, 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 (règlement nº 2252/2004), et des modèles types de visas [règlement (CE) nº 1683/95 du Conseil, du 29 mai 1995, établissant un modèle type de visa (JO 1995, L 164, p. 1)] ainsi que des titres de séjour pour les ressortissants de pays tiers (règlement nº 1030/2002), qui s'inspirent d'une approche cohérente du législateur de l'Union.

[63] Arrêt Schwarz (points 43 et 44), dans lequel la Cour a en outre considéré, en substance, que, s'il est exact que l'application de la méthode de vérification d'identité au moyen des empreintes digitales risque exceptionnellement de ne pas aboutir à des résultats optimaux, le défaut de concordance en ce qui concerne les données biométriques du titulaire aura normalement pour conséquence d'attirer l'attention des autorités compétentes sur la personne concernée et d'entraîner, à l'égard de celle-ci, un contrôle approfondi de cette personne destiné à établir son identité d'une manière définitive.

cause cette circonstance [64]. Même dans ce cas, la mise en place graduelle de cette mesure à l'égard des cartes nationales d'identité réduit le risque de falsification des documents nationaux et contribue progressivement à la réalisation de l'objectif du règlement 2019/1157.

87. En deuxième lieu, s'agissant de la question de savoir si le recueil et le stockage d'empreintes digitales dans les cartes d'identité sont également nécessaires, à savoir qu'il n'existe pas de méthode aussi appropriée, mais moins intrusive, pour atteindre le même objectif légitime, la juridiction de renvoi mentionne à titre principal deux autres options principales comme autres mesures possibles, dont la première fait l'objet d'un examen détaillé par la Commission dans l'analyse d'impact accompagnant la proposition de règlement [65].

88. En effet, la première option consisterait à limiter les exigences en matière de protection contre la falsification à une image faciale du titulaire de la carte, méthode qui servirait également à harmoniser les différentes normes de sécurité des cartes nationales d'identité au niveau national.

89. À cet égard, j'ai fait remarquer que la Cour a déjà jugé qu'une mesure de prélèvement d'empreintes digitales n'est pas une opération revêtant un caractère intime, comme c'est le cas pour les photos faciales. Elle est incapable d'entraîner un désagrément physique ou psychique particulier pour l'intéressé, à l'instar de la prise de sa photo faciale [66]. La Cour a en outre considéré que, même lorsque le prélèvement d'empreintes digitales s'ajoute à la prise de la photo faciale, le cumul de deux opérations destinées à l'identification des personnes ne peut a priori être considéré comme entraînant, en soi, une atteinte plus importante aux droits reconnus par les articles 7 et 8 de la Charte que si ces opérations étaient considérées isolément [67].

90. Par ailleurs, dès lors que les caractéristiques anatomiques du visage d'une personne peuvent évoluer de manière significative, en raison de diverses vicissitudes dans la vie de cette dernière, telles que le vieillissement ou l'apparition d'une maladie, la simple correspondance entre la photo faciale figurant sur la carte nationale d'identité et le visage du titulaire de la carte est davantage susceptible d'entraîner des erreurs d'identification que la vérification de la photo faciale figurant sur la carte nationale d'identité et des empreintes digitales de ce titulaire. À cet égard, ainsi que le relève le gouvernement allemand, même une correspondance biométrique de la photographie peut donner lieu à des erreurs en raison des techniques modernes de « morphing » qui consistent à fusionner plusieurs visages en une seule image faciale.

91. Par conséquent, une comparaison manuelle ou automatisée de l'image faciale figurant sur une carte nationale d'identité avec le visage du titulaire de la carte [68], qui est la méthode employée dans de nombreux États membres avant l'adoption du règlement 2019/1157, ne peut donner un résultat plus efficace que la combinaison des éléments d'identification biométriques visés à l'article 3, paragraphe 5, de ce règlement, à savoir une image faciale du titulaire de la carte et deux

64 Voir article 5 du règlement 2019/1157, qui prévoit que les cartes d'identité qui ne satisfont pas aux exigences énoncées à l'article 3 de ce règlement cessent d'être valides à leur expiration ou au plus tard le 3 août 2031, la date retenue étant la date la plus proche.

65 Voir l'analyse d'impact de la Commission (points 5.2 et 6.1) ainsi que le tableau 6.1, qui fait référence à l'« option ID 1 ». Cette option comprend un modèle présentant certaines caractéristiques communes telles que les informations sur la carte, les éléments de sécurité minimaux tenant compte de l'OACI Doc 9303 et une puce comportant une image faciale obligatoire.

66 Arrêt Schwarz (point 48).

67 Arrêt Schwarz (point 49).

68 En utilisant les systèmes EasyPass par exemple. Voir, à cet égard, le règlement (UE) 2017/2225 du Parlement européen et du Conseil, du 30 novembre 2017, modifiant le règlement (UE) 2016/399 en ce qui concerne l'utilisation du système d'entrée/de sortie (JO 2017, L 327, p. 1).

empreintes digitales [69]. À mon avis, il est possible de parvenir à une conclusion similaire si l'image faciale du titulaire était combinée uniquement à des hologrammes ou à des filigranes, comme le fait également valoir la juridiction de renvoi.

92. La seconde option serait de stocker une quantité plus faible de données dactyloscopiques sous forme de « points caractéristiques » ou d'exiger la prise d'une seule empreinte digitale. À cet égard, il importe de préciser que l'intégration de points caractéristiques dans les cartes nationales d'identité nécessiterait, dans un premier temps, la prise d'une empreinte digitale entière et, dans un second temps, l'extraction de ces points caractéristiques, ce qui implique qu'un traitement de données plus étendu devrait être effectué en plus du recueil et du stockage d'empreintes digitales individuelles. Pour cette raison, je ne pense pas que cette méthode puisse être considérée comme étant moins intrusive.

93. En outre, selon la littérature scientifique, le stockage de points caractéristiques ne semble pas offrir le même niveau de sécurité en matière de vérification d'identité que l'utilisation d'empreintes digitales complètes [70], ce qui constitue une considération qui peut s'ajouter aux préoccupations suscitées par l'utilisation de points caractéristiques en matière d'interopérabilité. À cet égard, ainsi que l'ont souligné la plupart des parties lors de l'audience, il n'existe pas de procédure uniforme établie, ni même de logiciel disponible, que ce soit au niveau européen ou national, pour lire des points caractéristiques à partir des cartes nationales d'identité, ce qui donnerait lieu à une charge insurmontable pour l'échange de données entre les autorités nationales [71].

94. Il en va de même, par exemple, pour la sphère internationale, où, afin que les cartes d'identité puissent être utilisées dans le transport aérien international, les spécifications du document 9303 de l'OACI doivent être respectées [72]. Ces spécifications établissent que, si un État prévoit l'intégration des empreintes digitales dans des documents de voyage lisibles à la machine, le stockage de l'image d'empreintes digitales est obligatoire pour permettre une interopérabilité globale [73]. Le stockage de points caractéristiques ne répond pas à ces exigences.

95. En ce qui concerne le prélèvement et le stockage d'une seule empreinte digitale, je suis encline à considérer que, bien que la quantité de données conservées soit inférieure à celle qui est conservée en cas de stockage de deux empreintes digitales, cette méthode n'est pas aussi adaptée, étant donné qu'elle aboutit à une moindre fiabilité. Le cas d'un prélèvement défectueux d'empreintes digitales ou d'une blessure du doigt dont l'empreinte a été prise peut être révélateur à cet égard. En tout état de cause, il ressort de la jurisprudence de la Cour que même le prélèvement d'un nombre plus élevé d'empreintes digitales peut être considéré comme proportionné [74].

[69] Voir l'analyse d'impact de la Commission, point 7.1 (p. 49), dans laquelle, après avoir comparé les différentes options en matière d'efficacité, elle conclut que la combinaison d'une image faciale et de deux empreintes digitales est plus efficace pour atteindre les objectifs spécifiques de réduction de la fraude documentaire et d'amélioration de l'authentification des documents. Voir également le point 7.4 (p. 56) de ce même document, selon lequel, aux fins d'améliorer l'acceptation des cartes nationales d'identité et, partant, de faciliter l'objectif de libre circulation, la combinaison d'une image faciale et de deux empreintes digitales est préférée à l'exigence d'une seule image faciale.

[70] Maltoni, D., e.a., *Handbook of Fingerprint Recognition*, 2^e édition, Springer, 2009, p. 53.

[71] En revanche, les États membres disposent d'instruments normalisés pour l'interopérabilité des éléments d'identification biométriques concernés par le règlement 2019/1157. Voir, à cet égard, article 3, paragraphe 6, de ce règlement et la décision C(2018) 7767 de la Commission.

[72] Voir considérant 23 du règlement 2019/1157.

[73] DOC 9303, *Documents de voyage lisibles à la machine*, 8^e édition (révision), OACI, 2021 (partie 9, chapitre 4).

[74] Même dix empreintes digitales peuvent être considérées comme proportionnées. Voir, en ce sens, arrêt du 3 octobre 2019, A e.a. (C-70/18, EU:C:2019:823, point 58).

96. Il résulte des considérations qui précèdent que, par rapport au prélèvement et au stockage d'empreintes digitales, une méthode tout aussi appropriée, mais moins intrusive, ne semble pas exister pour atteindre, de manière tout aussi efficace, l'objectif du règlement 2019/1157.

97. En troisième lieu, pour que l'article 3, paragraphe 5, du règlement 2019/1157 soit justifié au regard de l'objectif qu'il poursuit, encore faut-il que le traitement des empreintes digitales prélevées en vertu de cette disposition n'aille pas au-delà de ce qui est nécessaire pour atteindre cet objectif. À cet égard, le législateur doit s'assurer qu'il existe des garanties spécifiques visant à protéger ces données efficacement contre les traitements impropres et abusifs [75]. Cette justification ne peut être admise que si des limitations spécifiques à la menace en cause sont prévues afin d'empêcher tout abus [76].

98. En l'occurrence, il convient de souligner que l'article 3, paragraphes 5 et 6, ainsi que les articles 10 et 11 du règlement 2019/1157 prévoient un cadre juridique clair pour le recueil, le stockage et l'utilisation des éléments d'identification biométriques, à savoir les empreintes digitales [77].

99. En particulier, premièrement, les conditions régissant le recueil d'empreintes digitales sont énoncées à l'article 10 du règlement 2019/1157. Il est explicitement indiqué dans cette disposition que les éléments d'identification biométriques peuvent uniquement être recueillis par du personnel qualifié et dûment habilité désigné par les autorités chargées de délivrer les cartes d'identité, et uniquement dans le but d'être intégrés sur le support de stockage hautement sécurisé visé à l'article 3 de ce règlement. De plus, les États membres doivent veiller à ce que des procédures appropriées et efficaces soient en place pour le recueil des éléments d'identification biométriques, et ces procédures doivent respecter les droits et les principes énoncés non seulement dans la Charte, mais également dans la CEDH et la convention internationale des droits de l'enfant [78]. Ces procédures doivent également respecter, lorsque des difficultés se présentent, la dignité de la personne concernée.

100. Deuxièmement, en ce qui concerne le stockage des éléments d'identification biométriques après qu'ils ont été recueillis, il est expressément indiqué à l'article 3, paragraphe 6, du règlement 2019/1157 que le support de stockage des cartes nationales d'identité doit garantir l'intégrité, l'authenticité et la confidentialité des données, lesquelles doivent être sécurisées conformément aux instructions prévues dans la décision C(2018) 7767 de la Commission [79]. En outre, selon l'article 10, paragraphe 3, dudit règlement, le stockage d'éléments d'identification biométriques par les autorités publiques après qu'ils ont été recueillis est limité à la période comprise entre le recueil des données et la date de remise de la carte d'identité et, en tout état de cause, ne doit pas dépasser 90 jours à compter de la date de délivrance du document. Au cours de cette période, les données doivent être conservées de manière très sécurisée. Après ce délai, les empreintes digitales recueillies doivent être effacées ou détruites.

[75] Voir arrêt Schwarz (point 55). Voir également arrêt de la Cour EDH du 4 décembre 2008, S. et Marper c. Royaume-Uni (CE:ECHR:2008:1204JUD003056204, § 103).

[76] Arrêt du 8 avril 2014, Digital Rights Ireland e.a. (C-293/12 et C-594/12, EU:C:2014:238, points 54 et suiv.).

[77] Voir également considérant 22 du règlement 2019/1157.

[78] Adoptée par l'Assemblée générale des Nations unies le 20 novembre 1989, elle est entrée en vigueur le 2 septembre 1990.

[79] Voir, notamment, annexe III de la décision C(2018) 7767 de la Commission, point 5, sous l'intitulé « Data security and integrity issues » (problématiques liées à la sécurité et à l'intégrité des données).

101. Troisièmement, l'accès aux empreintes digitales stockées sur le support de stockage est également très limité au titre de l'article 11 du règlement 2019/1157. Seul le personnel dûment autorisé des autorités compétentes y a accès [80], et l'accès n'est possible que lorsque le droit de l'Union ou le droit national exige une carte d'identité. En outre, cet accès doit avoir pour seul but de vérifier l'authenticité de la carte d'identité et/ou l'identité du titulaire. Par ailleurs, la vérification de l'image faciale constitue l'objectif premier de la vérification de l'authenticité du document et de l'identité du titulaire, ce qui implique que, de manière générale, les États membres devraient vérifier les empreintes digitales uniquement lorsque c'est nécessaire pour confirmer sans aucun doute l'authenticité et l'identité [81].

102. À la lumière de ce qui précède, je considère que le règlement 2019/1157 offre des mesures suffisantes et appropriées qui garantissent que le recueil, le stockage et l'utilisation des éléments d'identification biométriques, en particulier des empreintes digitales, font l'objet d'une protection efficace contre les usages impropres et les abus.

103. Plus concrètement, ces mesures garantissent que les procédures de prélèvement sont effectuées par un personnel spécialisé en nombre réduit et qu'elles sont minutieusement mises en place à l'avance par les États membres afin de respecter les droits fondamentaux et la dignité des personnes concernées. Elles garantissent également que les éléments d'identification biométriques stockés dans une carte nouvellement émise restent à la seule disposition du titulaire de la carte après la remise de cette carte et qu'elles ne sont pas accessibles au public [82]. Les éléments d'identification biométriques sont conservés par les autorités publiques de manière très sécurisée uniquement en vue de délivrer la carte d'identité et aucun accès supplémentaire ou par d'autres personnes n'est autorisé. Les éléments d'identification biométriques doivent, en tout état de cause, être supprimés et détruits après une période de conservation par les autorités publiques clairement définie et raisonnable en cas de non-remise de la carte. Enfin, les mesures introduites par le règlement 2019/1157 confirment que les éléments d'identification biométriques sont accessibles et utilisés dans des circonstances strictement limitées, préétablies par la loi et dans l'unique but de vérifier l'authenticité de la carte et l'identité du titulaire, conformément à l'objectif principal de ce règlement.

104. Par souci d'exhaustivité, je souhaiterais renvoyer à la réserve qui figure au début de l'article 10, paragraphe 3, du règlement 2019/1157, qui a fait l'objet de plusieurs questions posées par la Cour lors de l'audience. Comme je l'ai déjà mentionné, avant de faire référence au stockage temporaire des empreintes digitales par les autorités publiques et à l'obligation de conserver ces éléments d'identification biométriques de manière très sécurisée, l'article 10, paragraphe 3, première phrase, de ce règlement contient la réserve suivante : « [s]auf s'ils sont nécessaires aux finalités du traitement dans le respect du droit de l'Union et du droit national ». Cette réserve

[80] Voir article 11, paragraphe 7, du règlement 2019/1157, qui exige également que les États membres communiquent chaque année à la Commission la liste des autorités compétentes ayant accès aux données biométriques. La Commission doit publier en ligne une compilation de ces listes nationales.

[81] Voir considérant 19 du règlement 2019/1157. Voir également article 4, paragraphe 3, du règlement n° 2252/2004, qui met en place une même utilisation limitée pour les passeports et documents de voyage.

[82] Comme la Commission l'a expliqué lors de l'audience, il résulte de la décision C(2018) 7767 de la Commission que, afin d'authentifier le terminal, la machine de lecture envoie son autorisation de lecture sous la forme de différents certificats numériques à la puce de la carte d'identité. La puce de la carte d'identité peut ainsi vérifier l'authenticité du certificat envoyé par le terminal. Cela signifie, dans la pratique, que seules les autorités compétentes énumérées à l'article 11, paragraphe 7, du règlement 2019/1157 peuvent avoir accès aux données biométriques, à l'exclusion de toute autre autorité ou personne.

semble découler de la négociation interinstitutionnelle – ou trilogue – qui s'est tenue entre le Parlement, le Conseil et la Commission au cours de la procédure législative ordinaire qui a donné lieu à l'adoption dudit règlement [83].

105. À cet égard, il est vrai que cette réserve pourrait laisser penser que les autorités publiques peuvent stocker des éléments d'identification biométriques, tels que les empreintes digitales, après leur prélèvement pendant une période plus longue que celle définie à l'article 10, paragraphe 3, du règlement 2019/1157 et que ces autorités peuvent les utiliser à des fins supplémentaires non définies de manière précise dans ce règlement, telles que, par exemple, l'établissement de bases de données nationales.

106. Toutefois, une lecture attentive de l'article 10, paragraphe 3, du règlement 2019/1157 révèle que cette réserve n'établit aucune base juridique pour d'autres objectifs que ceux spécifiquement prévus par ce règlement. En effet, cette réserve fait expressément référence à une législation supplémentaire, émanant soit de l'Union, soit des États membres, de sorte que toute limitation des droits garantis par les articles 7 et 8 de la Charte ne devrait être examinée qu'au regard de cette autre législation et non pas comme figurant de manière autonome dans ledit règlement. Cette lecture est particulièrement renforcée lorsque l'on examine le considérant 21 du même règlement [84], qui déclare sans ambiguïté que le règlement 2019/1157 ne fournit pas de base juridique pour la création ou la tenue à jour de bases de données au niveau national pour le stockage des données biométriques dans les États membres. Il revient au droit national de respecter le droit de l'Union en matière de protection des données. Ce même considérant ajoute que ce règlement ne constitue pas une base juridique pour la création ou la tenue à jour d'une base de données centralisée au niveau de l'Union.

107. C'est pour cette raison que je ne pense pas que la réserve qui figure au début de l'article 10, paragraphe 3, du règlement 2019/1157 soit susceptible de remettre en cause la conclusion énoncée au point 102 des présentes conclusions, selon laquelle ce règlement offre des garanties suffisantes pour empêcher que le traitement des éléments d'identification biométriques, en particulier les empreintes digitales, soit utilisé de façon impropre ou abusive.

108. Eu égard à ce qui précède, je conclurais que le règlement 2019/1157 et, en particulier, son article 3, paragraphe 5, ne constituent pas une limitation injustifiée aux articles 7 et 8 de la Charte, lus en combinaison avec l'article 52, paragraphe 1, de celle-ci.

109. Le deuxième motif soulevé par la juridiction de renvoi ne devrait pas conduire la Cour à déclarer l'invalidité du règlement 2019/1157.

[83] Voir le dossier interinstitutionnel du 22 février 2019, où il est déclaré que « le texte de compromis maintient tous les éléments clés du mandat de négociation du Conseil, et plus particulièrement : [...] la capacité des États membres à mettre en place et à maintenir des bases de données biométriques conformément à la législation nationale », disponible en anglais à l'adresse suivante : https://data.consilium.europa.eu/doc/document/ST-6412-2019-INIT/en/pdf.

[84] Voir également, à cet égard, l'analyse d'impact de la Commission, point 6 (p. 33 et 35), où il est indiqué que « rien dans ces initiatives ne fournira de base juridique pour le stockage centralisé des données collectées [...] ou pour l'utilisation de ces données à des fins autres que celle de vérifier l'authenticité du document et l'identité du titulaire », et que « toute mise en œuvre devra être compatible avec le droit de l'Union et les droits fondamentaux qu'il protège ».

C. Article 35, paragraphe 10, du RGPD

110. Par le troisième motif d'invalidité, la juridiction de renvoi se demande si l'article 3, paragraphe 5, du règlement 2019/1157 viole l'article 35, paragraphe 10, du RGPD. Faisant écho à la position adoptée par le CEPD dans son avis du 10 août 2018 [85], cette juridiction nourrit des doutes quant à la question de savoir si une analyse d'impact relative à la protection des données aurait dû être réalisée par le législateur de l'Union lors de l'adoption du règlement 2019/1157.

111. L'article 35 du RGPD figure au chapitre IV de celui-ci, intitulé « Responsable du traitement et sous-traitant », en particulier à la section 3, qui concerne l'analyse d'impact relative à la protection des données et la consultation préalable.

112. Selon l'article 35, paragraphe 1, du RGPD, lorsqu'un type de traitement, en particulier par le recours à de nouvelles technologies, est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, le responsable du traitement doit, avant le traitement, effectuer une analyse de l'impact des opérations de traitement envisagées sur la protection des données à caractère personnel. Les paragraphes 2 à 7 de cet article développent davantage le contenu de l'obligation des responsables du traitement d'effectuer une analyse d'impact, notamment en indiquant les cas dans lesquels cette évaluation est requise et en décrivant les éléments minimaux que cette analyse doit comporter.

113. En revanche, l'article 35, paragraphe 10, du RGPD établit une exception à l'obligation de procéder à une analyse d'impact, pour autant que les conditions énoncées à cette disposition soient remplies. Tel est notamment le cas lorsque i) le traitement des données est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis en vertu du droit de l'Union ou du droit national, ii) ce droit réglemente l'opération ou l'ensemble spécifique d'opérations de traitement en cause et iii) une analyse d'impact sur la protection des données a déjà été effectuée dans le cadre d'une analyse d'impact générale lors de l'adoption de ce droit.

114. En l'occurrence, je dois relever, d'emblée, que, même si la juridiction de renvoi cite l'article 35, paragraphe 10, du RGPD comme fondement de la violation concernée par le présent motif d'invalidité, les indications fournies dans l'ordonnance de renvoi suggèrent que ce motif est en réalité fondé sur la violation de l'article 35, paragraphe 1, du RGPD. C'est bien cette dernière disposition qui soumet les responsables du traitement, tels que définis à l'article 4, point 7, du RGPD, à l'obligation de procéder à une analyse d'impact lorsqu'il existe un risque élevé pour les droits et libertés des personnes physiques. Selon la juridiction de renvoi, c'est cette obligation qui s'imposait au législateur de l'Union lors de l'adoption du règlement 2019/1157 et qui semblerait, selon cette même juridiction, ne pas avoir été satisfaite.

115. En outre, il convient de relever que le RGPD et le règlement 2019/1157 sont des actes de droit dérivé qui, dans la hiérarchie des sources du droit de l'Union, occupent une place équivalente. Cela implique que, contrairement à ce qu'indique la juridiction de renvoi dans sa question, le RGPD ne saurait être considéré comme une « norme de rang supérieur » par rapport au règlement 2019/1157. À cet égard, il résulte, en substance, de la jurisprudence de la Cour que, à moins qu'un acte de droit dérivé ne contienne une disposition prévoyant expressément la

[85] Voir note en bas de page 11 des présentes conclusions.

primauté de l'un sur l'autre, la validité de ce dernier ne saurait être appréciée au regard du premier. Dans ce cas, il convient seulement d'assurer une application de chacun de ces actes qui soit compatible avec l'autre et en permettre ainsi une application cohérente [86].

116. S'agissant du règlement 2019/1157, je relève que ce règlement établit des liens explicites avec le RGPD, notamment à son article 11, en ce qui concerne la protection des données à caractère personnel. Cette disposition, qui devrait être lue à la lumière des considérants 40, 41 et 43 du règlement 2019/1157, fait apparaître que le RGPD s'applique en ce qui concerne les données à caractère personnel devant faire l'objet d'un traitement dans le cadre de l'application du règlement 2019/1157. Plus précisément, il découle de l'article 11, paragraphe 2, de ce règlement que les autorités chargées de la délivrance des cartes d'identité doivent être considérées comme le responsable du traitement visé à l'article 4, point 7, du RGPD et doivent être responsables du traitement des données à caractère personnel. En outre, l'article 11, paragraphe 3, du règlement 2019/1157 oblige les États membres à veiller à ce que les autorités de contrôle puissent exercer pleinement leurs missions visées dans le RGPD, y compris, par exemple, l'accès à toutes les données à caractère personnel ainsi que l'accès à tout local ou matériel de traitement des données des autorités compétentes.

117. Il découle du règlement 2019/1157 que le RGPD peut imposer des obligations aux organismes nationaux et aux autorités compétentes lors de la mise en œuvre du règlement 2019/1157. Les institutions de l'Union et les gouvernements intervenant devant la Cour admettent ce point. Cela étant, il ne résulte aucunement du RGPD que l'obligation de procéder à une analyse d'impact, telle que prévue à l'article 35, paragraphe 1, de celui-ci, lie le législateur de l'Union. Cette disposition n'établit pas non plus de critère au regard duquel, par exemple, la validité d'une autre norme du droit dérivé de l'Union devrait être évaluée.

118. À la lumière de ce qui précède, je conclus donc que l'article 35, paragraphe 1, du RGPD ne s'applique pas au législateur de l'Union lors de l'adoption d'une norme de droit dérivé et que, pour cette raison, le processus législatif ayant conduit à l'adoption du règlement 2019/1157 et, en particulier, de l'article 3, paragraphe 5, de ce règlement, ne saurait être considéré comme violant l'obligation de procéder à une analyse d'impact.

119. Il résulte des considérations qui précèdent que le troisième motif soulevé par la juridiction de renvoi ne devrait pas conduire la Cour à déclarer l'invalidité du règlement 2019/1157.

120. L'examen de la question posée par la juridiction de renvoi n'a révélé aucun élément de nature à affecter la validité du règlement 2019/1157 et, en particulier, de son article 3, paragraphe 5.

[86] Voir, en ce sens, arrêts du 29 juin 2010, Commission/Bavarian Lager (C-28/08 P, EU:C:2010:378, point 56), et du 28 juin 2012, Commission/Éditions Odile Jacob (C-404/10 P, EU:C:2012:393, point 110). Voir également conclusions de l'avocat général Pitruzzella dans les affaires jointes Luxembourg Business Registers (C-37/20 et C-601/20, EU:C:2022:43, point 66).

V. Conclusion

121. Eu égard à l'ensemble des considérations qui précèdent, je propose à la Cour de répondre à la question préjudicielle posée par le Verwaltungsgericht Wiesbaden (tribunal administratif de Wiesbaden, Allemagne) de la manière suivante :

L'examen de la question préjudicielle n'a révélé aucun élément de nature à affecter la validité 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, et notamment de son article 3, paragraphe 5.