Recueil de la jurisprudence

CONCLUSIONS DE L'AVOCAT GÉNÉRAL
M. PRIIT PIKAMÄE
présentées le 15 juin 2023[1]

**Affaire C-118/22**

**NG**
**Procédure administrative**
**contre**
**Direktor na Glavna direktsia „Natsionalna politsia" pri MVR – Sofia,**
**en présence de**
**Varhovna administrativna prokuratura**

[demande de décision préjudicielle formée par le Varhoven administrativen sad (Cour administrative suprême, Bulgarie)]

« Renvoi préjudiciel – Protection des personnes physiques à l'égard du traitement des données à caractère personnel – Directive (UE) 2016/680 – Articles 4, 5, 8, 10 et 16 – Conservation des données d'une personne physique condamnée pour une infraction intentionnelle jusqu'à son décès – Personne physique ayant été condamnée par un jugement définitif et ultérieurement réhabilitée – Rejet de la demande d'effacement – Nécessité et proportionnalité de l'ingérence dans les droits fondamentaux consacrés aux articles 7 et 8 de la charte des droits fondamentaux de l'Union européenne »

1. Faut-il s'inquiéter de la conservation des données à caractère personnel dans les fichiers de police enfermant l'individu inscrit, le cas échéant sa vie durant, dans un statut de déviant social, dangereux à perpétuité ? Ne faut-il pas, au contraire, se féliciter de cette mémoire policière au constat de la résolution par les enquêteurs d'affaires anciennes non élucidées, plus connues aujourd'hui sous le nom de « cold cases », pour le plus grand soulagement des familles de victimes ?

2. La présente affaire s'inscrit précisément dans ce questionnement antagoniste qui renvoie à la conciliation de l'intérêt public lié à la lutte contre la criminalité avec celui de l'individu tenant à la protection de ses données personnelles et au respect de sa vie privée. Elle donne l'occasion à la Cour de se prononcer sur la question du traitement de ces données à des fins répressives dans sa dimension temporelle, au regard des dispositions pertinentes de la directive (UE) 2016/680[2].

[1] Langue originale : le français.

[2] Directive du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil (JO 2016, L 119, p. 89).

## I. Le cadre juridique

### A. Le droit de l'Union

3. Sont pertinents dans le cadre de la présente affaire les articles 4, 5, 8, 10 et 16 de la directive 2016/680 ainsi que l'article 52, paragraphe 1, de la charte des droits fondamentaux de l'Union européenne (ci-après la « Charte »).

### B. Le droit bulgare

4. L'article 26, paragraphes 1 et 2, du zakon za Ministerstvo na vatreshnite raboti (loi relative au ministère de l'Intérieur, ci-après le « ZMVR ») dispose :

« (1) Lorsqu'elles traitent des données à caractère personnel en lien avec les activités de protection de la sécurité nationale, de lutte contre la criminalité, de maintien de l'ordre public et de conduite de procédures pénales, les autorités du ministère de l'Intérieur :

[...]

3. peuvent traiter toutes les catégories nécessaires de données à caractère personnel ;

[...]

(2) Les délais de conservation des données visées au paragraphe 1 ou de vérification périodique de la nécessité du stockage de celles-ci sont fixés par le ministre de l'Intérieur. Ces données sont également effacées en vertu d'un acte judiciaire ou d'une décision de la Commission de protection des données à caractère personnel. »

5. L'article 27 du ZMVR énonce :

« Les données provenant de l'inscription des personnes au registre de police effectuée sur la base de l'article 68 ne sont utilisées qu'à des fins de protection de la sécurité nationale, de lutte contre la criminalité et de maintien de l'ordre public. »

6. L'article 68 du ZMVR prévoit ce qui suit :

« (1) Les autorités de police inscrivent au registre de police les personnes qui sont poursuivies pour une infraction intentionnelle relevant de l'action publique. Les autorités chargées de l'instruction sont tenues de prendre les mesures nécessaires aux fins de l'inscription au registre par les autorités de police.

(2) L'inscription au registre de police est un type de traitement de données à caractère personnel des personnes visées au paragraphe 1, qui est effectué dans le cadre de la présente loi.

(3) Aux fins de l'inscription au registre de police, les autorités de police doivent :

1. collecter des données à caractère personnel relatives aux personnes visées à l'article 18 de la loi relative aux documents d'identité bulgares ;

2. relever les empreintes digitales des personnes et photographier celles-ci ;

3. effectuer des prélèvements aux fins du profilage ADN des personnes.

[...]

(6) L'inscription au registre de police est radiée sur la base d'un ordre écrit du responsable du traitement de données à caractère personnel ou des fonctionnaires habilités par celui-ci, d'office ou à la suite d'une demande écrite et motivée de la personne inscrite, lorsque :

1. l'enregistrement a été effectué en violation de la loi ;

2. la procédure pénale est classée, sauf dans les cas visés à l'article 24, paragraphe 3, du [Nakazatelno-protsesualen kodeks (code de procédure pénale)] ;

3. la procédure pénale a abouti à un acquittement ;

4. la personne a été exonérée de sa responsabilité pénale et une sanction administrative lui a été infligée ;

5. la personne est décédée, auquel cas la demande peut être faite par ses héritiers.

(7) Les modalités d'inscription au registre de police et de radiation de cette inscription sont déterminées par un règlement du Conseil des ministres. »

## II. Les faits à l'origine du litige, la procédure au principal et la question préjudicielle

7. NG a fait l'objet d'une inscription au fichier de police, effectuée dans le cadre d'une procédure d'instruction, pour faux témoignage, infraction pénale prévue à l'article 290, paragraphe 1, du Nakazatelen Kodeks (code pénal). À la suite de cette procédure, un acte d'accusation a été dressé, le 2 juillet 2015, contre lui, et, par jugement du 28 juin 2016, confirmé en appel par jugement du 2 décembre 2016, il a été reconnu coupable et condamné à une peine de probation d'un an. La peine a été purgée le 14 mars 2018.

8. Le 15 juillet 2020, NG a présenté une demande de radiation de cette inscription auprès de l'administration territoriale compétente du Ministerstvo na vatreshnite raboti (ministère de l'Intérieur, Bulgarie), en produisant un extrait de son casier judiciaire certifiant qu'il n'était pas condamné.

9. Par décision du 2 septembre 2020, l'autorité administrative compétente a rejeté cette demande au motif qu'une condamnation par jugement définitif ne fait pas partie des motifs de radiation de l'inscription au fichier de police, énumérés de manière exhaustive à l'article 68, paragraphe 6, du ZMVR, y compris en cas de réhabilitation, au sens de l'article 85 du code pénal. Le 8 octobre 2020, NG a formé un recours contre cette décision devant l'Administrativen sad Sofia grad (tribunal administratif de la ville de Sofia, Bulgarie). Par décision du 2 février 2021, cette juridiction a rejeté ce recours.

10. NG a formé un pourvoi contre la décision de l'Administrativen sad Sofia grad (tribunal administratif de la ville de Sofia) devant le Varhoven administrativen sad (Cour administrative suprême, Bulgarie). Le principal moyen du pourvoi est tiré d'une méconnaissance du principe, qui se déduirait des articles 5, 13 et 14 de la directive 2016/680, selon lequel le traitement de données à caractère personnel par stockage ne saurait avoir une durée illimitée. Or, en l'absence de motif de radiation de l'inscription au fichier de police, une personne condamnée ne pourrait pas demander, après sa réhabilitation, l'effacement de ses données collectées en lien avec l'infraction pénale pour laquelle elle a purgé sa peine, de sorte que la durée de stockage de celles-ci serait illimitée.

11. Éprouvant des doutes quant à la conformité de la réglementation nationale régissant le fichier de police en cause avec le droit de l'Union, la juridiction de renvoi a décidé de surseoir à statuer dans le litige au principal et de poser à la Cour la question préjudicielle suivante :

« L'interprétation de l'article 5 de la [directive 2016/680], lu conjointement avec l'article 13, paragraphe 2, sous b), et l'article 13, paragraphe 3, de cette directive, s'oppose-t-elle à des mesures législatives nationales qui conduiraient à un droit quasi illimité au traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales et/ou à une perte par la personne concernée de son droit à la limitation du traitement, à l'effacement ou la destruction de ses données ? »

## III. La procédure devant la Cour

12. Les gouvernements bulgare, tchèque, irlandais, espagnol et polonais ainsi que la Commission européenne ont présenté des observations écrites. Lors de l'audience qui s'est tenue le 7 février 2023, ont également été entendus en leurs observations orales la partie demanderesse au principal, les gouvernements bulgare, irlandais, espagnol, néerlandais et polonais ainsi que la Commission.

## IV. Analyse

### A. Sur l'applicabilité de la directive 2016/680

13. Il ressort de la demande de décision préjudicielle que la juridiction de renvoi tient manifestement pour acquis que la réglementation nationale litigieuse relève du champ d'application ratione materiae de la directive 2016/680, position me paraissant justifier quelques observations.

14. Conformément à une lecture combinée de l'article 1er, paragraphe 1, et de l'article 2, paragraphe 1, de la directive 2016/680, cette dernière s'applique au traitement de données à caractère personnel effectué par les autorités compétentes aux fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces. L'article 2, paragraphe 3, sous a), de la directive 2016/680 exclut de son champ d'application le traitement de données à caractère personnel effectué « dans le cadre d'une activité qui ne relève pas du champ d'application du droit de l'Union ». Les considérants 12 et 14 de cette directive précisent la teneur de cette exception d'inapplicabilité en indiquant qu'elle

couvre notamment les activités relatives à la sécurité nationale, à la différence de celles concernant le maintien de l'ordre public lorsque cette mission est confiée à la police ou à d'autres autorités répressives lorsque cela est nécessaire à des fins de protection contre les menaces pour la sécurité publique et pour les intérêts fondamentaux de la société protégés par la loi, et de prévention de telles menaces, qui sont susceptibles de déboucher sur une infraction pénale.

15. Interprétant l'article 2, paragraphe 2, sous a), du règlement (UE) 2016/679 [3] prévoyant une exception à l'applicabilité de ce règlement libellée en des termes identiques à ceux de l'article 2, paragraphe 3, sous a), de la directive 2016/680, la Cour a jugé que cette première disposition, lue à la lumière du considérant 16 dudit règlement, doit être considérée comme ayant pour seul objet d'exclure du champ d'application de cette norme les traitements de données à caractère personnel effectués par les autorités étatiques dans le cadre d'une activité qui vise à préserver la sécurité nationale ou d'une activité pouvant être rangée dans la même catégorie, de telle sorte que le seul fait qu'une activité soit propre à l'État ou à une autorité publique ne suffit pas pour que cette exception soit automatiquement applicable à une telle activité. Elle a précisé que les activités qui ont pour but de préserver la sécurité nationale couvrent, en particulier, celles ayant pour objet de protéger les fonctions essentielles de l'État et les intérêts fondamentaux de la société [4].

16. Or, en l'occurrence, les données enregistrées et conservées par la police au titre de l'article 68 du ZMVR le sont, conformément à l'article 27 de cette loi, aux fins de la protection de la sécurité nationale, de la lutte contre la criminalité et du maintien de l'ordre public. Il apparaît ainsi que le fichier de police en cause constitue une base de données unique et hybride, car regroupant des informations pouvant faire l'objet de traitements répondant à des finalités distinctes dont celle tenant à la protection de la sécurité nationale, qui ne relève pas du champ d'application matériel de la directive 2016/680. Dans ces circonstances, la licéité de la conservation des données figurant dans un tel fichier ne peut être examinée au regard des exigences de cette directive pour autant que ces données sont utilisées aux seules fins visées à l'article 1er, paragraphe 1, de ladite directive, ce qu'il incombe à la juridiction de renvoi de vérifier [5]. En l'état du dossier soumis à la Cour, il n'apparaît pas que la conservation des données de NG dans le fichier de police, dont il demande l'effacement, puisse être considérée comme un traitement échappant au champ d'application matériel de la directive 2016/680.

17. Il importe, à ce stade, de souligner que la réglementation nationale en cause dans l'affaire au principal a déjà fait l'objet d'un arrêt de la Cour faisant suite à l'interrogation d'une juridiction bulgare chargée d'apprécier le refus d'une personne mise en examen au titre d'une infraction de fraude fiscale de se soumettre à la collecte de ses données. La Cour s'y est notamment prononcée sur la licéité de la collecte des données par rapport aux exigences de l'article 10 de la directive 2016/680, jugeant que ce dernier, lu en combinaison avec l'article 4, paragraphe 1, sous a) à c), ainsi qu'avec l'article 8, paragraphes 1 et 2, de cette directive, doit être interprété en ce sens qu'il s'oppose à une législation nationale qui prévoit la collecte systématique des données

[3] 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 »).

[4] Voir, en ce sens, arrêt du 22 juin 2021, Latvijas Republikas Saeima (Points de pénalité) (C-439/19, EU:C:2021:504, points 61 à 67). Dans l'arrêt du 5 avril 2022, Commissioner of An Garda Síochána e.a. (C-140/20, EU:C:2022:258, point 61), la Cour a précisé que l'objectif de préservation de la sécurité nationale correspond à l'intérêt primordial de protéger les fonctions essentielles de l'État et les intérêts fondamentaux de la société, par la prévention et la répression des activités de nature à déstabiliser gravement les structures constitutionnelles, politiques, économiques ou sociales fondamentales d'un pays, et en particulier à menacer directement la société, la population ou l'État en tant que tel, telles que notamment des activités de terrorisme.

[5] Une telle vérification peut paraître, il est vrai, délicate à mettre en œuvre en pratique en présence d'un fichier de police unique « attrape-tout », l'enregistrement et la conservation des données obéissant à une logique à la fois rétrospective et prospective ne se prêtant pas nécessairement à une différenciation objective des traitements en cause sur la base d'une finalité bien précise.

biométriques et génétiques de toute personne mise en examen pour une infraction intentionnelle poursuivie d'office aux fins de leur enregistrement, sans prévoir l'obligation, pour l'autorité compétente, de vérifier et de démontrer, d'une part, si cette collecte est absolument nécessaire à la réalisation des objectifs concrets poursuivis et, d'autre part, si ces objectifs ne peuvent pas être atteints par des mesures constituant une ingérence de moindre gravité pour les droits et les libertés de la personne concernée[6]. La présente affaire conduit la Cour à devoir examiner la licéité d'une ingérence distincte, à savoir la *conservation* des informations se rapportant aux personnes physiques pénalement condamnées identifiées par leurs prénom et nom dans le fichier de police en cause, laquelle constitue un traitement de données à caractère personnel effectué par une autorité publique compétente à des fins de prévention et de détection des infractions pénales et d'enquêtes, soit le ministère de l'Intérieur bulgare, au sens de l'article 3, paragraphes 1 et 2, et de l'article 3, paragraphe 7, sous a), de la directive 2016/680.

## B. Sur la reformulation de la question préjudicielle

18. À titre liminaire, il convient de rappeler que, dans le cadre de la procédure de coopération entre les juridictions nationales et la Cour instituée à l'article 267 TFUE, il appartient à celle-ci de donner au juge national une réponse utile qui lui permette de trancher le litige dont il est saisi. Dans cette optique, il incombe, le cas échéant, à la Cour de reformuler les questions qui lui sont soumises. En effet, la Cour a pour mission d'interpréter toutes les dispositions du droit de l'Union dont les juridictions nationales ont besoin afin de statuer sur les litiges qui leur sont soumis, même si ces dispositions ne sont pas indiquées expressément dans les questions qui lui sont adressées par ces juridictions[7].

19. Les faits de l'affaire au principal ont trait à une demande de radiation de l'inscription au fichier de police de données à caractère personnel, formée par une personne physique qui, après avoir été condamnée pour faux témoignage, a purgé sa peine et a été réhabilitée le 14 mars 2020, soit près de cinq ans après l'inscription susmentionnée. Cette demande a été rejetée par décision de l'autorité administrative compétente, confirmée en première instance par la décision de l'Administrativen sad Sofia grad (tribunal administratif de la ville de Sofia), laquelle fait l'objet d'un pourvoi devant la juridiction de renvoi qui éprouve des doutes quant à la compatibilité de la réglementation nationale avec la directive 2016/680 en ce qui concerne la question de la conservation des données dans le fichier de police. L'affaire au principal concerne donc à l'évidence le droit à l'effacement des données à caractère personnel dans les meilleurs délais, tel que prévu à l'article 16, paragraphe 2, de la directive 2016/680, lorsque le traitement constitue une violation des dispositions adoptées en vertu des articles 4, 8 ou 10 de celle-ci ou lorsque ces données doivent être effacées pour respecter une obligation légale à laquelle est soumis le responsable du traitement.

6 Arrêt du 26 janvier 2023, Ministerstvo na vatreshnite raboti (Enregistrement de données biométriques et génétiques par la police) (C-205/21, EU:C:2023:49, point 135). Je relève que la Cour s'est préalablement prononcée sur une question de compatibilité de l'article 52, paragraphe 1, de la Charte avec la réglementation bulgare qui présente la particularité de se référer au RGPD et avec une disposition de droit interne transposant l'article 10 de la directive 2016/680, sans que cette dernière ne soit formellement visée. La Cour a jugé que le traitement de données biométriques et génétiques par les autorités de police en vue de leurs activités de recherche, « à des fins de lutte contre la criminalité et de maintien de l'ordre public », est autorisé par le droit d'un État membre, au sens de l'article 10, sous a), de cette directive, dès lors que le droit de cet État membre contient une base juridique suffisamment claire et précise pour autoriser ledit traitement, la double référence susmentionnée n'étant pas de nature, en soi, à remettre en cause l'existence d'une telle autorisation, pour autant qu'il ressort, de manière suffisamment claire, précise et dénuée d'équivoque de l'interprétation de l'ensemble des dispositions applicables du droit national, que le traitement des données biométriques et génétiques en cause relève du champ d'application de cette directive, et non du RGPD.

7 Arrêt du 8 mai 2019, PI (C-230/18, EU:C:2019:383, point 42).

20. L’article 4, paragraphe 1, sous c) et e), de la directive 2016/680 dispose que les États membres doivent s’assurer que les données à caractère personnel sont, conformément aux principes respectivement de minimisation de ces données et de limitation de leur conservation, adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont traitées et conservées sous une forme permettant l’identification des personnes concernées pendant une durée n’excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées [8]. Quant à l’article 8 de cette directive, il est consacré à la licéité du traitement, laquelle est conditionnée par la nécessité d’un traitement effectué aux fins de l’exécution d’une mission par une autorité compétente, pour les finalités énoncées à l’article 1er, paragraphe 1, de ladite directive, et d’une base juridique européenne ou nationale, cette dernière devant préciser au moins les objectifs du traitement, les données à caractère personnel devant faire l’objet d’un traitement et les finalités du traitement. Enfin, s’agissant de l’article 10 de la directive 2016/680, il détermine le régime juridique du traitement portant sur des catégories particulières de données à caractère personnel, telles que les données biométriques et génétiques utilisées dans le fichier de police aux fins d’identifier une personne physique de manière unique.

21. Force est de constater que les dispositions évoquées au point précédent ne sont pas visées dans la question préjudicielle alors qu’elles sont manifestement pertinentes aux fins de la réponse que la Cour est appelée à fournir en l’espèce. La juridiction de renvoi a sollicité l’interprétation de l’article 5, de l’article 13, paragraphe 2, sous b), et paragraphe 3, de la directive 2016/680 qui ne font pas partie des dispositions expressément mentionnées par l’article 16, paragraphe 2, de cette directive dont la violation par la réglementation nationale justifie la mise en œuvre du droit à l’effacement accordé à la personne concernée. Toutefois, ce droit est également reconnu lorsque les données doivent être effacées pour respecter une obligation légale à laquelle est soumis le responsable du traitement, ce qui est susceptible de correspondre aux situations envisagées à l’article 5 et à l’article 13, paragraphe 2, sous b), de ladite directive, à savoir et respectivement : la fixation de délais maximum de conservation des données ou d’examens périodiques de la nécessité d’une telle conservation [9] et la fourniture par le responsable du traitement à la personne concernée, dans des cas particuliers, d’informations additionnelles à celles visées au paragraphe 1 de l’article 13 afin de lui permettre d’exercer ses droits. En revanche, le paragraphe 3 de cet article 13 concerne la possibilité pour les États membres d’adopter, sous certaines conditions, des mesures législatives visant à retarder ou à limiter la fourniture des informations à la personne concernée en application du paragraphe 2, voire à ne pas les fournir, ce qui ne peut pas relever d’une obligation légale imposée au responsable du traitement.

22. En tout état de cause, il ne ressort pas de la décision de renvoi que se soit posée dans l’affaire au principal la question de l’information de NG quant à ses droits, l’intéressé ayant manifestement pu les exercer comme le démontre le recours dont il a saisi les autorités administratives puis judiciaires concernant la conservation de ses données. La question adressée à la Cour ne paraît donc pas requérir l’interprétation de l’article 13, paragraphe 2, sous b), et paragraphe 3, de la directive 2016/680. Partant, ce sont en particulier l’article 16, paragraphe 2, de la directive 2016/680 ainsi que les articles 4, 5, 8 et 10 de celle-ci qui sont en cause dans l’affaire au principal.

[8] Le respect de l’article 4, paragraphe 1, sous b), de la directive 2016/680, selon lequel les données sont collectées pour des finalités déterminées, explicites et légitimes et ne sont pas traitées d’une manière incompatible avec ces finalités, ne fait pas débat en l’espèce, dans la mesure où l’objectif du traitement ultérieur à la collecte des données que constitue la conservation de celles-ci est identique à celui de la collecte.

[9] L’article 26 de la ZMVR énonce que les délais de conservation des données à caractère personnel ou de vérification périodique de la nécessité du stockage de celles-ci sont fixés par le ministre de l’Intérieur. À l’audience, le gouvernement bulgare a indiqué qu’une telle vérification a lieu tous les trois mois.

23. Par ailleurs, ainsi que l'énonce son considérant 104, la directive 2016/680 respecte les droits fondamentaux et observe les principes reconnus par la Charte, tels qu'ils sont consacrés par le traité sur le fonctionnement de l'Union européenne, et notamment le droit au respect de la vie privée et familiale et le droit à la protection des données à caractère personnel. Selon le considérant 46 de cette directive, toute limitation des droits de la personne concernée doit respecter la Charte et la convention européenne des droits de l'homme et des libertés fondamentales, signée à Rome le 4 novembre 1950 (ci-après la « CEDH »), telles qu'elles sont interprétées respectivement par la Cour et par la Cour européenne des droits de l'homme (ci-après la « Cour EDH ») dans leur jurisprudence, et notamment respecter l'essence desdits droits et libertés. Il convient de rappeler que les droits fondamentaux au respect de la vie privée et à la protection des données à caractère personnel, garantis par les articles 7 et 8 de la Charte, ne sont pas des prérogatives absolues, mais doivent être pris en considération par rapport à leur fonction dans la société et être mis en balance avec d'autres droits fondamentaux. Des limitations peuvent ainsi être apportées, pourvu que, conformément à l'article 52, paragraphe 1, de la Charte, elles soient prévues par la loi et qu'elles respectent le contenu essentiel des droits fondamentaux ainsi que le principe de proportionnalité. En vertu de ce dernier principe, des limitations ne peuvent être apportées que si elles sont nécessaires et répondent effectivement à des objectifs d'intérêt général reconnus par l'Union ou au besoin de protection des droits et des libertés d'autrui. Elles doivent s'opérer dans les limites du strict nécessaire et la réglementation comportant l'ingérence doit prévoir des règles claires et précises régissant la portée et l'application de la mesure en cause [10].

24. Dans ces conditions, il y a lieu de considérer que la juridiction de renvoi demande, en substance, si les articles 4, 5, 8, 10 et l'article 16, paragraphe 2, de la directive 2016/680, lus de manière combinée et à la lumière de l'article 52, paragraphe 1, de la Charte, doivent être interprétés en ce sens qu'ils s'opposent à une législation nationale prévoyant la conservation de données à caractère personnel dans un fichier de police, incluant les données biométriques et génétiques de la personne concernée, jusqu'au décès de celle-ci, et ne lui permettant pas d'obtenir l'effacement de ces données à la suite de la réhabilitation dont elle a bénéficié postérieurement à sa condamnation pénale [11].

## C. Sur la conservation des données à caractère personnel à des fins répressives

25. Avant d'examiner la compatibilité de la réglementation nationale concernant le fichier de police en cause, il m'apparaît nécessaire d'envisager la problématique de la conservation des données à des fins répressives à l'aune de certaines dispositions de la directive 2016/680 ainsi que de la jurisprudence de la Cour et de la Cour EDH.

26. En premier lieu, il convient de relever que la directive 2016/680 vise à contribuer à la réalisation d'un espace de liberté, de sécurité et de justice au sein de l'Union, tout en mettant en place un cadre pour la protection des données à caractère personnel solide et cohérent afin d'assurer le respect du droit fondamental de la protection des personnes physiques à l'égard du traitement des données à caractère personnel, reconnu à l'article 8, paragraphe 1, de la Charte et à l'article 16, paragraphe 1, TFUE, ce droit étant étroitement lié au droit au respect de la vie privée,

[10] Arrêt du 22 juin 2021, Latvijas Republikas Saeima (Points de pénalité) (C-439/19, EU:C:2021:504, point 105).

[11] Je relève que l'article 18 de la directive 2016/680, selon lequel les États membres peuvent prévoir que les droits visés, notamment à l'article 16, sont exercés conformément au droit d'un État membre lorsque les données à caractère personnel figurent dans une décision judiciaire ou un casier ou dossier judiciaire faisant l'objet d'un traitement lors d'une enquête judiciaire et d'une procédure pénale, ne me paraît pas pertinent, le fichier en cause constituant un outil visant à faciliter l'activité opérationnelle des services d'enquête dont le responsable est le ministre de l'Intérieur et non un instrument judiciaire à proprement parler, du type de ceux mentionnés ci-dessus.

consacré à l'article 7 de la Charte [12]. À cette fin, les chapitres II et III de la directive 2016/680 énoncent, respectivement, les principes régissant les traitements des données à caractère personnel ainsi que les droits de la personne concernée que doit respecter tout traitement de telles données. En particulier, tout traitement de données à caractère personnel doit être conforme aux principes relatifs au traitement des données et aux conditions de licéité du traitement énoncés aux articles 4 et 8 de cette directive. Les exigences contenues dans cette dernière disposition constituant une expression de celles découlant de l'article 52, paragraphe 1, de la Charte, elles doivent être interprétées à la lumière de cet article [13].

27. Dans la réponse à fournir à la juridiction de renvoi, il y a donc lieu de tenir compte du principe de la « minimisation des données » énoncé à l'article 4, paragraphe 1, sous c), de la directive 2016/680 qui donne expression au principe de proportionnalité [14]. Il en va de même du principe de limitation de la conservation, contenu à l'article 4, paragraphe 1, sous e), de cette directive, lequel implique de procéder à une appréciation du caractère proportionné du traitement par rapport à sa finalité, au regard de l'écoulement du temps. Contreviendra à ce principe la conservation des données pendant une durée excédant celle nécessaire, c'est-à-dire allant au-delà de la durée nécessaire à la réalisation des finalités pour lesquelles ces données ont été conservées [15]. Il en résulte que même un traitement initialement licite de données peut devenir, avec le temps, incompatible avec la directive 2016/680 lorsque ces données ne sont plus nécessaires à la réalisation de telles finalités et qu'elles doivent être supprimées lorsque lesdites finalités sont réalisées [16].

28. La problématique temporelle de la conservation des données est également abordée à l'article 5 de la directive 2016/680 sous la forme d'un complément et d'une précision aux exigences de son article 4 [17]. Ainsi que le mentionne le considérant 26 de ladite directive, afin de garantir que les données ne soient pas conservées plus longtemps que nécessaire, des délais doivent être fixés par le responsable du traitement en vue de leur effacement ou d'un examen périodique. Force est de constater que l'article 5 de la directive 2016/680, d'une part, laisse aux États membres le soin d'apprécier et de fixer la durée pertinente de conservation et, d'autre part, envisage la vérification régulière de la nécessité de conserver les données comme une alternative à la fixation a priori d'une période de conservation maximum. Cette seconde observation me paraît revêtir une importance certaine dans la présente affaire, car elle traduit la reconnaissance par le législateur de l'Union d'une possible conservation à durée indéfinie des données à des fins répressives [18]. Cette constatation doit être reliée avec les termes de l'article 16, paragraphe 3, de la

12 Voir, en ce sens, arrêts du 25 février 2021, Commission/Espagne (Directive données à caractère personnel – Domaine pénal) (C-658/19, EU:C:2021:138, point 75), et du 1er août 2022, Vyriausioji tarnybinės etikos komisija (C-184/20, EU:C:2022:601, point 61).

13 Voir, par analogie, arrêt du 1er août 2022, Vyriausioji tarnybinės etikos komisija (C-184/20, EU:C:2022:601, points 62 et 69).

14 Voir, par analogie, arrêt du 22 juin 2021, Latvijas Republikas Saeima (Points de pénalité) (C-439/19, EU:C:2021:504, point 98).

15 Voir, en ce sens, arrêts du 7 mai 2009, Rijkeboer (C-553/07, EU:C:2009:293, point 33), et du 13 mai 2014, Google Spain et Google (C-131/12, EU:C:2014:317, point 92).

16 Voir, par analogie, arrêt du 20 octobre 2022, Digi (C-77/21, EU:C:2022:805, point 54).

17 Cette problématique est également envisagée au considérant 26 et à l'article 4, paragraphe 3, de la directive 2016/680 dont il ressort que le législateur de l'Union a envisagé une possible conservation de longue durée de données faisant l'objet d'un archivage dans l'intérêt public, à des fins scientifiques, statistiques ou historiques, aux fins énoncées à l'article 1er, paragraphe 1, de cette directive, sous réserve de garanties appropriées pour les droits et libertés de la personne concernée. Telle n'est pas la situation en l'espèce, la conservation des données dans le fichier de police ayant une finalité purement opérationnelle, à savoir faciliter l'activité des services d'enquête aux fins d'élucidation des infractions.

18 On peut se demander si l'article 5 de la directive 2016/680 ne recèle pas une forme de contradiction logique intrinsèque. En effet, il peut donc y avoir, conformément à cette disposition, des données à caractère personnel traitées par les services répressifs pour lesquelles il ne serait pas approprié de prévoir des délais aux fins de leur effacement mais il est requis, dans une telle situation de conservation temporellement indéfinie, de prévoir une vérification régulière par les autorités compétentes de la nécessité de conserver ces données et une possibilité d'effacement, si la conservation n'est plus justifiée au regard de la finalité du traitement. On peut, toutefois, comprendre et admettre que l'objectif, légitime, est de prévoir un correctif destiné à prévenir les abus dans la mise en œuvre d'un dispositif intrusif.

directive 2016/680, qui envisage la possibilité de limiter le traitement des données comme alternative à leur effacement, notamment, à son point b), lorsque les données à caractère personnel doivent être conservées « à des fins probatoires », ce qui démontre qu'il n'existe pas de droit absolu à l'effacement [19].

29. La question de la licéité de la conservation des données inclut nécessairement celle de leur nature, qui recouvre en l'occurrence, notamment, les empreintes digitales, des photographies, un prélèvement ADN de la personne suspectée d'avoir commis une infraction ou condamnée pénalement à ce titre, ce type de données faisant entrer le traitement dans le champ d'application de l'article 10 de la directive 2016/680. Il importe de souligner que, si le régime juridique défini par cette disposition ne comporte pas, à la différence de celui prévu à l'article 9 du RGPD, d'interdiction de principe d'un traitement portant sur de telles données, ce dernier est autorisé « uniquement en cas de nécessité absolue », sous réserve de garanties appropriées pour les droits et libertés de la personne concernée, et lorsqu'ils sont, notamment, autorisés par le droit de l'Union ou le droit d'un État membre.

30. Selon la jurisprudence, la finalité de l'article 10 de la directive 2016/680 est d'assurer une protection accrue à l'égard de ces traitements qui, en raison de la sensibilité particulière des données en cause et du contexte dans lequel elles sont traitées, sont susceptibles d'engendrer, ainsi qu'il ressort du considérant 37 de cette directive, des risques importants pour les libertés et les droits fondamentaux, tels que le droit au respect de la vie privée et le droit à la protection des données à caractère personnel, garantis par les articles 7 et 8 de la Charte. Ainsi qu'il résulte des termes mêmes dans lesquels elle est énoncée à l'article 10 de la directive 2016/680, l'exigence selon laquelle le traitement de telles données est autorisé « uniquement en cas de nécessité absolue » doit être interprétée comme définissant des conditions renforcées de licéité du traitement des données sensibles, au regard de celles qui découlent de l'article 4, paragraphe 1, sous b) et c), et de l'article 8, paragraphe 1, de cette directive, lesquelles se réfèrent seulement à la « nécessité » d'un traitement de données relevant, de manière générale, du champ d'application de ladite directive. Ainsi, d'une part, l'emploi de l'adverbe « uniquement » devant l'expression « en cas de nécessité absolue » souligne que le traitement de catégories particulières de données, au sens de l'article 10 de la directive 2016/680, ne pourra être considéré comme nécessaire que dans un nombre limité de cas. D'autre part, le caractère « absolu » de la nécessité d'un traitement de telles données implique que cette nécessité soit appréciée de manière particulièrement rigoureuse [20].

31. En deuxième lieu, je relève que si la Cour s'est déjà prononcée à plusieurs reprises sur la question de la licéité de la conservation des données à des fins répressives, elle l'a fait dans des contextes normatifs et factuels singulièrement distincts de celui de la présente affaire. Ainsi, la

[19] La présente affaire concerne un refus total d'effacement dont les motifs doivent être fournis au requérant selon l'article 16, paragraphe 4, de la directive 2016/680, lequel prévoit, cependant, que les États membres peuvent adopter des mesures législatives limitant cette obligation en tout ou en partie, notamment pour éviter de nuire à la prévention ou à la détection d'infractions pénales, aux enquêtes ou aux poursuites en la matière.

[20] Arrêt du 26 janvier 2023, Ministerstvo na vatreshnite raboti (Enregistrement de données biométriques et génétiques par la police) (C-205/21, EU:C:2023:49, points 116 à 118). Eu égard à ces considérations, faut-il comprendre que la Cour conditionne la licéité du traitement des données sensibles dans le cadre de la directive 2016/680 au respect d'un critère allant au-delà de celui habituellement retenu pour tout type de données dans la jurisprudence de la Cour en matière de protection des données personnelles, tenant au respect des limites du « strict nécessaire » par le traitement en cause ? En réponse à une observation du gouvernement français sur le fait que, dans certaines versions linguistiques, l'article 10 de la directive 2016/680 se réfère aux cas où le traitement de données est « strictement nécessaire », la Cour a répondu, au point 119 de cet arrêt, que cette variation terminologique ne modifie pas la nature du critère ainsi visé et le niveau d'exigence requis, dès lors que ces versions linguistiques définissent également une condition renforcée pour que soit autorisé le traitement de données sensibles, impliquant une appréciation plus rigoureuse de sa nécessité que dans le cas où les données traitées ne relèvent pas du champ d'application dudit article. Reste qu'on peut s'interroger sur cette distinction conceptuelle dans le degré d'intensité de la nécessité du traitement et la difficulté de sa mise en œuvre dans une affaire donnée.

Cour a jugé [21] que le droit de l'Union issu de la directive 2002/58/CE [22], dont il résulte que les utilisateurs des moyens de communication électroniques sont en droit de s'attendre, en principe, à ce que leurs communications et les données y afférentes restent, en l'absence de leur consentement, anonymes et ne puissent pas faire l'objet d'un enregistrement, s'oppose à une conservation généralisée et indifférenciée, à titre préventif, des données de trafic et de localisation aux fins de lutte contre la criminalité, quel que soit son degré de gravité, cette conservation n'étant admise, sous certaines conditions, qu'en cas de menace grave, réelle et actuelle ou prévisible pour la sécurité nationale. Elle a ajouté que le droit de l'Union ne s'oppose pas, en revanche, à des mesures prévoyant, aux fins de la lutte contre la criminalité grave, une conservation généralisée et indifférenciée des données relatives à l'identité civile des utilisateurs et, pour une période temporellement limitée au strict nécessaire, de leurs adresses IP, à une conservation ciblée des données délimitée, sur la base d'éléments objectifs et non discriminatoires, en fonction de catégories de personnes concernées ou au moyen d'un critère géographique, pour une période temporellement limitée au strict nécessaire, mais renouvelable et, à la conservation rapide des données relatives dont disposent les fournisseurs de services pour une durée déterminée, toutes ces mesures devant assurer, par des règles claires et précises, que la conservation des données en cause est subordonnée au respect des conditions matérielles et procédurales y afférentes et que les personnes concernées disposent de garanties effectives contre les risques d'abus.

32. La Cour a également fait usage du critère tenant au respect des limites du strict nécessaire pour le traitement des données personnelles dans le contexte du transfert, de la conservation et de l'utilisation des données contenues dans les dossiers des passagers de vols extra-UE constitués par les transporteurs aériens (ci-après les « données PNR »), en vue de la prévention et de la détection des infractions terroristes et des formes graves de criminalité [23]. La Cour a eu l'occasion de souligner que la durée de conservation des données PNR pouvant, conformément à l'accord PNR UE-Canada, aller jusqu'à cinq ans, cet accord permet de disposer d'informations sur la vie privée des passagers aériens sur une durée particulièrement longue et que, s'agissant des passagers aériens pour lesquels un risque en matière de terrorisme ou de criminalité transnationale grave n'a pas été identifié à leur arrivée au Canada et jusqu'à leur départ de ce pays tiers, il n'apparaît pas exister, une fois qu'ils sont repartis, de rapport, ne serait-ce qu'indirect, entre leurs données PNR et l'objectif poursuivi par l'accord envisagé, qui justifierait la conservation de ces données. Elle a donc conclu qu'un stockage continu des données PNR de l'ensemble des passagers aériens après leur départ du Canada aux fins d'un accès éventuel auxdites données, indépendamment d'un lien quelconque avec la lutte contre le terrorisme et la criminalité transnationale grave, n'était pas justifié [24].

33. La Cour s'est prononcée, dans le cadre d'un renvoi préjudiciel, sur la validité et l'interprétation de la directive (UE) 2016/681 [25] qui oblige les transporteurs aériens à transférer les données de tout passager empruntant un vol extra-UE, opéré entre un pays tiers et l'Union européenne, à l'unité d'information passagers de l'État membre de destination ou de départ du vol concerné, afin de

[21] Voir, notamment, arrêts du 6 octobre 2020, La Quadrature du Net e.a. (C-511/18, C-512/18 et C-520/18, EU:C:2020:791), et du 5 avril 2022, Commissioner of An Garda Síochána e.a. (C-140/20, EU:C:2022:258).

[22] Directive du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques) (JO 2002, L 201, p. 37).

[23] Avis 1/15 (Accord PNR UE-Canada), du 26 juillet 2017 (EU:C:2017:592), et arrêt du 21 juin 2022, Ligue des droits humains (C-817/19, EU:C:2022:491).

[24] Avis 1/15 (Accord PNR UE-Canada), du 26 juillet 2017 (EU:C:2017:592), points 132, 204 et 205).

[25] Directive du Parlement européen et du Conseil du 27 avril 2016 relative à l'utilisation des données des dossiers passagers (PNR) pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière (JO 2016, L 119, p. 132).

lutter contre le terrorisme et les formes graves de criminalité. Les données PNR ainsi transférées font l'objet d'une évaluation préalable par l'unité d'information passagers durant une période de six mois et sont ensuite conservées pendant cinq ans en vue d'une éventuelle évaluation postérieure par les autorités compétentes des États membres, ce qui peut conduire à des analyses effectuées pendant une période considérable, voire indéfinie, s'agissant des personnes qui voyagent par avion plus d'une fois tous les cinq ans. La Cour a considéré que cette directive comporte des ingérences d'une gravité certaine dans les droits garantis aux articles 7 et 8 de la Charte, dans la mesure, notamment, où elle vise à instaurer un régime de surveillance continu, non ciblé et systématique, incluant l'évaluation automatisée de données à caractère personnel de l'ensemble des personnes faisant usage des services de transport aérien, tout en se prêtant à une interprétation conforme aux articles 7, 8 et 21 ainsi qu'à l'article 52, paragraphe 1, de la Charte. La Cour a précisé que, après l'expiration de la période de conservation initiale de six mois, la conservation des données PNR n'apparaît pas limitée au strict nécessaire en ce qui concerne les passagers aériens pour lesquels ni l'évaluation préalable, ni les éventuelles vérifications effectuées au cours de la période de conservation initiale de six mois, ni aucune autre circonstance n'ont révélé l'existence d'éléments objectifs de nature à établir un risque en matière d'infractions terroristes ou de formes graves de criminalité présentant un lien objectif, à tout le moins indirect, avec le voyage aérien effectué par ces passagers. En revanche, elle a estimé que, au cours de la période initiale de six mois, la conservation des données PNR de l'ensemble des passagers aériens soumis au système instauré par ladite directive ne paraît pas, par principe, excéder les limites du strict nécessaire.

34. Par opposition à la jurisprudence rappelée ci-dessus, il importe de souligner, d'une part, que, contrairement à ce qui est établi en matière de traitement des données dans la directive 2002/58 [26], le consentement de la personne concernée ne constitue pas une base juridique pour le traitement des données à caractère personnel effectué par les autorités compétentes aux fins des finalités énoncées à l'article 1er, paragraphe 1, de la directive 2016/680. Ainsi qu'il est précisé au considérant 35 de celle-ci, dans le cadre de l'exécution des missions de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales qui leur sont confiées de manière institutionnelle par la loi, les autorités compétentes peuvent demander ou *ordonner* aux personnes physiques de donner suite aux demandes qui leur sont adressées. D'autre part, il n'est pas question dans la présente affaire de la conservation et de l'analyse automatisée d'un « océan de données » [27] générées dans le secteur des communications électroniques ou celui du transport aérien, stockées par des opérateurs privés et transférées à des services d'investigation, mais d'un fichier de police unique contenant les données de personnes pour lesquelles il existe des motifs sérieux de croire qu'elles ont commis une infraction, soupçonnées et condamnées pénalement, sous le contrôle exclusif d'une autorité publique et strictement confidentiel.

35. La spécificité du contexte normatif et factuel de la jurisprudence précitée empêche, selon moi, toute transposition pure et simple des solutions y retenues pour répondre à la présente question préjudicielle, s'agissant particulièrement de la distinction entre les objectifs de conservation des données (sauvegarde de la sécurité nationale, lutte contre la criminalité grave ou contre des infractions ne relevant pas de cette dernière) et la corrélation nécessaire entre l'importance de ces objectifs et le degré de gravité des ingérences dans les droits fondamentaux pouvant être

[26] Arrêt du 5 avril 2022, Commissioner of An Garda Síochána e.a. (C-140/20, EU:C:2022:258, points 35 à 37). Il en va de même en ce qui concerne la comparaison avec le régime juridique prévu par le RGPD.

[27] Tinière, R., *Jurisprudence de la CJUE 2020 : décisions et commentaires*, Bruylant, Bruxelles, 2021, p. 130 à 139.

justifiées [28]. Dit autrement, l'énonciation selon laquelle la lutte contre la criminalité en général peut uniquement justifier des ingérences ne présentant pas un caractère grave [29] ne peut être retenue en l'espèce, sous peine de réduire grandement l'effet utile de la directive 2016/680 et des instruments nationaux d'enquête/de sécurité publique, tels que le fichier de police en cause, relevant du champ d'application de cette norme dont l'objet exprime précisément la nécessité de pouvoir traiter, de manière proportionnée, des données à des fins policières. Il y a lieu de relever que, ainsi qu'il ressort des considérants 10 et 11 de la directive 2016/680, le législateur de l'Union a entendu adopter des règles qui tiennent compte de la nature spécifique du domaine couvert par cette directive. À cet égard, le considérant 12 énonce que les activités menées par la police ou d'autres autorités répressives sont axées principalement sur la prévention et la détection d'infractions pénales, sans autre précision, les enquêtes et les poursuites en la matière, y compris les activités de police effectuées sans savoir au préalable si un incident constitue une infraction pénale ou non [30].

36. En troisième lieu, il convient de relever que l'article 7 de la Charte, relatif au droit au respect de la vie privée et familiale, contient des droits correspondant à ceux garantis à l'article 8, paragraphe 1, de la CEDH, et que la protection des données a' caractère personnel joue un rôle fondamental pour l'exercice du droit au respect de la vie privée et familiale consacré à l'article 8 de la CEDH. En conséquence, il y a lieu, conformément à l'article 52, paragraphe 3, de la Charte, de donner audit article 7 le même sens et la même portée que ceux conférés à l'article 8, paragraphe 1, de la CEDH, tel qu'interprété par la jurisprudence de la Cour EDH [31].

37. La Cour EDH considère que la protection des données à caractère personnel joue un rôle fondamental dans l'exercice du droit au respect de la vie privée consacré à l'article 8 de la CEDH et que le simple fait de mémoriser des données relatives à la vie privée d'un individu constitue une ingérence au sens de cet article 8, peu importe que les informations mémorisées soient ou non utilisées par la suite. Selon cette juridiction, le droit interne doit notamment assurer que ces données sont pertinentes et non excessives par rapport aux finalités pour lesquelles elles sont enregistrées, et qu'elles sont conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire aux finalités pour lesquelles elles sont enregistrées. Le droit interne doit aussi contenir des garanties aptes à protéger efficacement les données à caractère personnel enregistrées contre les usages impropres et abusifs, tout en offrant une possibilité concrète de présenter une requête en effacement des données mémorisées. La Cour EDH a pris soin, cependant, de préciser qu'elle a pleinement conscience que, pour protéger leur population comme elles en ont le devoir, les autorités nationales sont amenées à constituer des fichiers contribuant efficacement à la répression et à la prévention de certaines infractions, *notamment* les plus graves. Toutefois, de tels dispositifs ne sauraient être mis en œuvre dans une logique excessive de maximalisation des informations qui y sont placées et de la durée de leur conservation [32]. Sur ce dernier point, la Cour EDH considère que l'absence d'une période maximum pour la conservation des données personnelles des personnes condamnées

[28] Arrêts du 5 avril 2022, Commissioner of An Garda Síochána e.a. (C-140/20, EU:C:2022:258, points 56 à 59), et du 21 juin 2022, Ligue des droits humains (C-817/19, EU:C:2022:491, point 148).

[29] Arrêt du 21 juin 2022, Ligue des droits humains (C-817/19, EU:C:2022:491, point 148).

[30] Voir, en ce sens, arrêt du 8 décembre 2022, Inspektor v Inspektorata kam Visshia sadeben savet (Finalités du traitement de données à caractère personnel – Enquête pénale) (C-180/21, EU:C:2022:967, points 57 et 58).

[31] Arrêt du 8 décembre 2022, Google (Déréférencement d'un contenu prétendument inexact) (C-460/20, EU:C:2022:962, point 59).

[32] Cour EDH, 22 juin 2017, Aycaguer c. France (CE:ECHR:2017:0622JUD000880612, §§ 33, 34 et 38), et Cour EDH, 18 septembre 2014, Brunet c. France (CE:ECHR:2014:0918JUD002101010, § 35).

n'est pas nécessairement incompatible avec l'article 8 de la CEDH, mais que l'existence et le fonctionnement de certaines garanties procédurales sont d'autant plus nécessaires dans cette hypothèse [33].

## D. Sur l'ingérence dans les droits fondamentaux garantis aux articles 7 et 8 de la Charte

38. Ainsi qu'il ressort de l'article 68 du ZMVR et des observations présentées par le gouvernement bulgare lors de l'audience, les données visées par la réglementation nationale comprennent, notamment, l'état civil de la personne concernée, les faits répréhensibles que cette dernière est suspectée avoir commis ou pour lesquels elle a été condamnée pénalement, ses empreintes digitales, des photographies, des prélèvements ADN aux fins de profilage. Dès lors que ces données comportent ainsi des informations sur des personnes physiques identifiées, les différents traitements dont elles peuvent faire l'objet affectent le droit fondamental au respect de la vie privée, garanti à l'article 7 de la Charte. En outre, les traitements de ces données, tels que ceux prévus par la réglementation nationale, relèvent également de l'article 8 de la Charte en raison du fait qu'ils constituent des traitements de données à caractère personnel au sens de cet article et doivent, par suite, nécessairement satisfaire aux exigences de protection des données prévues audit article [34].

39. À l'instar de la Cour EDH selon laquelle le simple fait de mémoriser des données relatives à la vie privée d'un individu constitue une ingérence au sens de l'article 8 de la CEDH [35], la Cour considère que la conservation des données constitue, par elle-même, une ingérence dans les droits fondamentaux au respect de la vie privée et à la protection des données à caractère personnel, consacrés aux articles 7 et 8 de la Charte, sans qu'il importe de savoir si les informations relatives à la vie privée concernées présentent ou non un caractère sensible, si les intéressés ont ou non subi d'éventuels inconvénients en raison de cette ingérence, ou encore si les données conservées seront ou non utilisées par la suite [36].

40. En ce qui concerne la gravité de l'ingérence que constitue la conservation, elle est avérée au regard de la nature de certaines données, s'agissant particulièrement des données biométriques et génétiques figurant dans le fichier de police, la Cour ayant qualifié d'importants les risques que représente le traitement des données sensibles pour les droits et les libertés des personnes concernées, en particulier dans le contexte des missions des autorités compétentes aux fins énoncées à l'article 1er, paragraphe 1, de la directive 2016/680 [37]. À cet égard, il est précisé au considérant 23 de cette directive que, compte tenu du caractère complexe et sensible des informations génétiques, le risque est grand que le responsable du traitement fasse un usage abusif et réutilise des données à diverses fins. Quant au considérant 51 de ladite directive, il énonce que des risques pour les droits et libertés des personnes physiques peuvent résulter du traitement de données qui pourraient entraîner des dommages physiques matériels ou un préjudice moral, notamment, lorsque des données génétiques ou biométriques sont traitées afin d'identifier une personne de manière unique ou lorsque des données relatives à des condamnations pénales et à des infractions sont traitées.

[33] Cour EDH, 4 juin 2013, Peruzzo et Martens c. Allemagne (CE:ECHR:2013:0604DEC000784108, § 46), et Cour EDH, 13 février 2020, Gaughran c. Royaume-Uni (CE:ECHR:2020:0213JUD004524515, § 88).

[34] Voir, par analogie, avis 1/15 (Accord PNR UE-Canada), du 26 juillet 2017 (EU:C:2017:592, points 122 et 123), et arrêt du 21 juin 2022, Ligue des droits humains (C-817/19, EU:C:2022:491, points 94 et 95).

[35] Cour EDH, 22 juin 2017, Aycaguer c. France (CE:ECHR:2017:0622JUD000880612, § 33).

[36] Voir, par analogie, arrêt du 5 avril 2022, Commissioner of An Garda Síochána e.a. (C-140/20, EU:C:2022:258, point 44).

[37] Arrêt du 26 janvier 2023, Ministerstvo na vatreshnite raboti (Enregistrement de données biométriques et génétiques par la police) (C-205/21, EU:C:2023:49, point 127).

41. La durée de conservation des données au fichier de police concourt aussi au constat de la gravité de l'ingérence, en ce sens que cette conservation est possible la vie durant de la personne condamnée pénalement. Enfin, il résulte de l'article 26, paragraphe 6, du ZMVR que les données personnelles peuvent être transférées à des autorités compétentes et des destinataires des États membres de l'Union, des organes et agences de l'Union, des pays tiers ou des organisations internationales. Il convient, à cet égard, de rappeler que la directive 2016/680 a pour but de faciliter le libre flux des données à caractère personnel entre les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces au sein de l'Union, et le transfert de telles données vers des pays tiers et à des organisations internationales, afin de garantir l'efficacité de la coopération judiciaire en matière pénale et de la coopération policière [38]. Rappelons, à cet égard, que le droit à la protection des données à caractère personnel exige, notamment, que la continuité du niveau élevé de protection des libertés et des droits fondamentaux conféré par le droit de l'Union soit assurée en cas de transfert de données à caractère personnel depuis l'Union vers un pays tiers [39].

42. Eu égard à l'ensemble des considérations qui précèdent, il convient de conclure que la réglementation nationale en cause au principal comporte des ingérences d'une gravité certaine dans les droits garantis aux articles 7 et 8 de la Charte dans la mesure, notamment, où elle vise à instaurer un instrument de conservation continue de données sensibles, susceptibles de franchir les frontières de l'État concerné, des personnes condamnées pénalement.

## E. Sur la justification de l'ingérence

43. Ainsi qu'il a été exposé, les droits fondamentaux consacrés aux articles 7 et 8 de la Charte n'apparaissent pas comme étant des prérogatives absolues et il ressort de l'article 52, paragraphe 1, de la Charte que celle-ci admet des limitations à l'exercice de ces droits, pour autant que ces limitations soient prévues par la loi, qu'elles respectent le contenu essentiel desdits droits et que, dans le respect du principe de proportionnalité, elles soient 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 [40]. Selon le considérant 26 de la directive 2016/680, les autorités répressives peuvent mener des activités à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces, pour autant qu'elles soient déterminées par la loi et qu'elles constituent une mesure nécessaire et proportionnée dans une société démocratique, en tenant dûment compte des intérêts légitimes de la personne physique concernée.

44. En ce qui concerne le respect du principe de proportionnalité, il convient de rappeler que la protection du droit fondamental au respect de la vie privée exige, conformément à une jurisprudence constante de la Cour, que les dérogations à la protection des données à caractère personnel et les limitations de celle-ci s'opèrent dans les limites du strict nécessaire étant entendu que, lorsqu'un choix s'offre entre plusieurs mesures appropriées à la satisfaction des objectifs légitimes poursuivis, il convient de recourir à la moins contraignante. En outre, un objectif d'intérêt général ne saurait être poursuivi sans tenir compte du fait qu'il doit être concilié avec les

[38] Voir considérants 4 et 7 de la directive 2016/680.

[39] Avis 1/15 (Accord PNR UE-Canada), du 26 juillet 2017 (EU:C:2017:592, point 134).

[40] Arrêt du 6 octobre 2020, Privacy International (C-623/17, EU:C:2020:790, points 63 et 64).

droits fondamentaux concernés par la mesure, et ce en effectuant une pondération équilibrée entre, d'une part, l'objectif d'intérêt général et, d'autre part, les droits en cause, afin de s'assurer que les inconvénients causés par cette mesure ne soient pas démesurés par rapport aux buts visés. Ainsi, la possibilité de justifier une limitation aux droits garantis aux articles 7 et 8 de la Charte doit être appréciée en mesurant la gravité de l'ingérence que comporte une telle limitation et en vérifiant que l'importance de l'objectif d'intérêt général poursuivi par cette limitation est en relation avec cette gravité [41].

### *1. Sur le respect du principe de légalité*

45. L'exigence selon laquelle toute limitation de l'exercice des droits fondamentaux doit être prévue par la loi implique que la base légale qui permet l'ingérence dans ces droits doit définir elle-même la portée de la limitation de l'exercice du droit concerné. À cet égard, la Cour a jugé, en outre, que la réglementation comportant une mesure permettant une telle ingérence doit prévoir des règles claires et précises régissant la portée et l'application de la mesure en cause et imposant des exigences minimales, de telle sorte que les personnes dont les données à caractère personnel ont été transférées disposent de garanties suffisantes permettant de protéger efficacement ces données contre les risques d'abus. Par conséquent, la base juridique de tout traitement de données à caractère personnel relevant du champ d'application de la directive 2016/680 doit, ainsi que le législateur de l'Union l'a, au demeurant, souligné au considérant 33 de celle-ci, être claire et précise et son application être prévisible pour les justiciables. En particulier, ces derniers doivent être en mesure d'identifier les circonstances et les conditions dans lesquelles la portée des droits que leur confère ladite directive est susceptible de faire l'objet d'une limitation [42].

46. L'examen de la réglementation nationale en cause, fournie dans la décision de renvoi complétée par les observations du gouvernement bulgare, permet, selon moi, de considérer que l'exigence tenant à la « qualité » de la loi est satisfaite, étant rappelé que cette dernière n'exclut pas que la limitation en cause soit formulée dans des termes suffisamment ouverts pour pouvoir s'adapter à des cas de figure différents ainsi qu'aux changements de situations [43].

47. Il apparaît ainsi que l'inscription et la conservation des données dans le fichier de police ont pour finalités exhaustives, selon l'article 27 de la ZMVR, la protection de la sécurité nationale, la lutte contre la criminalité et le maintien de l'ordre public, ce traitement visant à faciliter l'activité d'enquête opérationnelle décrite de manière détaillée à l'article 8 de cette loi [44]. La portée du traitement quant à la nature des infractions en relevant, aux données concernées, aux conditions de leur recueil, aux fonds d'informations dans lesquels elles sont traitées et à la durée de leur conservation est fixée avec suffisamment de précision à l'article 68 de la ZMVR et à l'article 28 du Naredba za reda za izvarshvane i snemane na politseyska registratsia (règlement relatif aux modalités d'inscription au registre de police et de radiation de cette inscription, ci-après le « NRISPR »). La réglementation nationale prévoit, explicitement et conformément au considérant 26 de la directive 2016/680, des procédures pour garantir l'intégrité et la

[41] Voir, en ce sens, arrêts du 6 octobre 2020, Privacy International (C-623/17, EU:C:2020:790, point 67), et du 22 novembre 2022, Luxembourg Business Registers (C-37/20 et C-601/20, EU:C:2022:912, point 64).

[42] Arrêts du 6 octobre 2020, Privacy International (C-623/17, EU:C:2020:790, point 65), et du 24 février 2022, Valsts ieņēmumu dienests (Traitement des données personnelles à des fins fiscales) (C-175/20, EU:C:2022:124, points 54 à 56). Il est vrai qu'un tel examen a trouvé sa place dans des arrêts de la Cour dans le cadre d'une analyse circonstanciée de la proportionnalité de la limitation, lorsqu'il n'est pas conjointement envisagé sous les deux angles liés au respect des principes de légalité et de proportionnalité [arrêt du 21 juin 2022, Ligue des droits humains (C-817/19, EU:C:2022:491, points 114 et 117)]. Je m'attacherai dans cette partie des présentes conclusions à la vérification de l'exigence de prévisibilité stricto sensu.

[43] Arrêt du 21 juin 2022, Ligue des droits humains (C-817/19, EU:C:2022:491, point 114).

[44] Voir points 33 à 35 des observations du gouvernement bulgare.

confidentialité des données à caractère personnel ainsi que la destruction de celles-ci au travers des informations fournies à la personne concernée, conformément aux articles 54 et 55 du zakon za zashtita na lichnite danni (loi relative à la protection des données à caractère personnel), notamment quant aux droits de celle-ci de demander au responsable du traitement l'accès aux données, leur rectification ou leur effacement. À cet égard, les motifs de radiation, la procédure et les effets afférents à cette dernière sont précisés à l'article 68 du ZMVR et aux articles 18 et suivants du NRISPR. Ces dispositions sont libellées avec suffisamment de précision et de clarté pour permettre aux destinataires de la loi de régler leur conduite et répondent ainsi à l'exigence de prévisibilité dégagée de la jurisprudence de la Cour EDH [45].

### *2. Sur le respect du contenu essentiel des droits fondamentaux garantis aux articles 7 et 8 de la Charte*

48. En ce qui concerne le contenu essentiel du droit fondamental au respect de la vie privée, consacré à l'article 7 de la Charte, la nature des informations contenues dans le fichier de police est limitée à un aspect spécifique de cette vie privée, relatif au passé pénal de la personne concernée, ce qui ne permet pas de tirer des conclusions concernant, de manière générale, la vie privée de cette personne, tels ses habitudes de la vie quotidienne, ses lieux de séjour permanents ou temporaires, ses déplacements journaliers ou autres, les activités exercées, ses relations sociales et les milieux sociaux fréquentés par celle-ci et, ainsi, d'établir son profil. Quant au contenu essentiel du droit à la protection des données à caractère personnel, consacré à l'article 8 de la Charte, les développements qui précèdent révèlent que la réglementation nationale en cause circonscrit les finalités du traitement des données et prévoit une énumération exhaustive des données conservées et des règles destinées à assurer leur accès, rectification ou effacement. Dans ces conditions, l'ingérence que comporte la conservation des données prévue par cette réglementation ne porte pas atteinte au contenu essentiel des droits fondamentaux consacrés aux articles susmentionnés [46].

### *3. Sur l'objectif d'intérêt général et l'aptitude du traitement des données en cause au regard de cet objectif*

49. Ainsi qu'il a été constaté dans les présentes conclusions, les données provenant de l'inscription des personnes au fichier de police effectuée sur la base de l'article 68 du ZMVR sont utilisées à des fins de protection de la sécurité nationale, de lutte contre la criminalité et de maintien de l'ordre public. Le gouvernement bulgare a indiqué que les données sont recueillies et traitées aux fins de la procédure pénale dans le cadre de laquelle la personne concernée a été mise en examen ainsi que pour être confrontées à d'autres données collectées lors d'enquêtes relatives à d'autres infractions. Cette dernière finalité concerne également la confrontation avec des données collectées dans d'autres États membres [47].

50. Ce traitement relève, selon ce gouvernement, de l'activité d'enquête opérationnelle décrite à l'article 8 du ZMVR dont les finalités sont définies comme suit : la prévention et la détection des infractions pénales, des menaces à la sécurité nationale et des atteintes à l'ordre public ; la recherche de personnes qui se soustraient à leur responsabilité pénale ou qui se sont soustraites à

[45] Voir, en ce sens, arrêt du 20 mai 2003, Österreichischer Rundfunk e.a. (C-465/00, C-138/01 et C-139/01, EU:C:2003:294, point 77).

[46] Voir, par analogie, Avis 1/15 (Accord PNR UE-Canada), du 26 juillet 2017 (EU:C:2017:592, point 150), et, a contrario, arrêt du 22 novembre 2022, Luxembourg Business Registers (C-37/20 et C-601/20, EU:C:2022:912, point 51).

[47] Arrêt du 26 janvier 2023, Ministerstvo na vatreshnite raboti (Enregistrement de données biométriques et génétiques par la police) (C-205/21, EU:C:2023:49, point 99).

l'exécution d'une peine dans des affaires pénales relevant de l'action publique, ainsi que la recherche de personnes disparues ; la recherche d'objets qui sont l'objet ou l'instrument de la commission d'une infraction pénale ou qui peuvent servir de preuves, ainsi que la préparation et la conservation des preuves matérielles et leur présentation aux autorités judiciaires compétentes.

51. La Cour a précisé que l'objectif de protection de la sécurité publique constitue un objectif d'intérêt général de l'Union susceptible de justifier des ingérences, même graves, dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte. Au demeurant, une telle protection contribue également à la protection des droits et des libertés d'autrui. À cet égard, l'article 6 de la Charte énonce le droit de toute personne non seulement à la liberté, mais également à la sûreté, cette disposition garantissant des droits correspondant à ceux qui le sont à l'article 5 de la CEDH [48]. Dans l'affaire portant sur la compatibilité de la collecte des données répertoriées dans le même fichier de police bulgare, la Cour a clairement jugé que ce traitement concernant des personnes mises en examen dans le cadre d'une procédure pénale aux fins de leur enregistrement poursuit les finalités énoncées à l'article 1er, paragraphe 1, de la directive 2016/680, en particulier celles relatives à la prévention et à la détection d'infractions pénales ainsi qu'aux enquêtes et aux poursuites en la matière, lesquelles constituent des objectifs d'intérêt général reconnus par l'Union. Elle a ajouté qu'une telle collecte est susceptible de contribuer à l'objectif énoncé au considérant 27 de la directive 2016/680, selon lequel, aux fins de la prévention des infractions pénales ainsi que des enquêtes et des poursuites en la matière, les autorités compétentes ont besoin de traiter des données à caractère personnel, collectées dans le cadre de la prévention et de la détection d'infractions pénales spécifiques, ainsi que des enquêtes et des poursuites en la matière au-delà de ce cadre, pour acquérir une meilleure compréhension des activités criminelles et établir des liens entre les différentes infractions pénales mises au jour [49]. Ces considérations valent bien évidemment pour la mesure de conservation des données.

52. Le fait que la conservation des données dans le fichier de police soit un traitement permettant d'atteindre les objectifs d'intérêt général de détection et, par voie de conséquence, de prévention des infractions pénales me paraît difficilement contestable. Il est évident qu'un fichier de police comportant les identités civiles, les photographies, les données biométriques et génétiques – et donc les caractéristiques physiques d'une personne uniques et infalsifiables –, des individus recensés constitue un outil d'enquête pleinement pertinent pour les services de sécurité aux fins de l'élucidation des infractions et l'identification de leurs auteurs. En ce sens, la réglementation nationale en cause répond à des critères objectifs, établissant un rapport entre les données à conserver et l'objectif poursuivi [50].

### *4. Sur le caractère nécessaire et proportionné de l'ingérence en cause*

53. Si la conservation des données dans le fichier de police en cause est manifestement apte à réaliser l'objectif d'intérêt général poursuivi, il reste à vérifier si l'ingérence dans les droits garantis aux articles 7 et 8 de la Charte, qui résulte d'une telle conservation, est limitée au strict nécessaire, en ce sens que l'objectif ne pourrait raisonnablement être atteint de manière aussi

[48] Avis 1/15 (Accord PNR UE-Canada), du 26 juillet 2017 (EU:C:2017:592, point 149), et arrêt du 6 octobre 2020, La Quadrature du Net e.a. (C-511/18, C-512/18 et C-520/18, EU:C:2020:791, point 123).

[49] Arrêt du 26 janvier 2023, Ministerstvo na vatreshnite raboti (Enregistrement de données biométriques et génétiques par la police) (C-205/21, EU:C:2023:49, points 97 et 98). La Cour EDH a relevé, dans le contexte de l'obligation positive découlant de l'article 2 de la CEDH, que l'intérêt public à enquêter et éventuellement à obtenir la poursuite et la condamnation des auteurs d'actes illicites, plusieurs années après les faits, a été fermement reconnu (Cour EDH, 12 juin 2014, Jelić c. Croatie, CE:ECHR:2014:0612JUD005785611, § 52).

[50] Voir, en ce sens, arrêt du 5 avril 2022, Commissioner of An Garda Síochána e.a. (C-140/20, EU:C:2022:258, point 55).

efficace par d'autres moyens moins attentatoires à ces droits fondamentaux des personnes concernées, et si elle n'est pas disproportionnée par rapport à cet objectif, ce qui implique notamment une pondération de l'importance de celui-ci et de la gravité de ladite ingérence [51].

54. Dans l'exercice de ce contrôle, il y a lieu de tenir compte, dans le cas présent, de l'objet du fichier de police, de la nature des infractions concernées et du nombre de personnes susceptibles d'y être inscrites, de la sensibilité particulière des données personnelles recueillies et de la durée de leur conservation, des garanties juridiques et/ou techniques prévues par la réglementation nationale pour la consultation du fichier et le contrôle du maintien des données dans celui-ci.

### *a) Sur l'objet du fichier*

55. Dans ses observations écrites, le gouvernement irlandais a fait valoir, en substance, que la conservation des données pouvait être nécessaire à des fins de contrôle connexe, servant l'intérêt public en matière de prévention de la criminalité et de sauvegarde de la sécurité publique. Ainsi, les informations contenues dans un fichier de police devraient pouvoir être consultées, non seulement pour rechercher les auteurs d'infractions mais également à des fins de police administrative, dans le cadre d'enquêtes préalables à des décisions de recrutement ou d'habilitation concernant certains emplois publics ou sensibles, le but étant de vérifier que le comportement des intéressés n'est pas incompatible avec l'exercice de ces fonctions.

56. Lors de l'audience, le gouvernement bulgare a confirmé ce qui pouvait être déduit du libellé explicite de l'article 27 du ZMVR, à savoir que le fichier de police en cause est un outil d'aide aux enquêtes judiciaires et non administratives. Cette constatation revêt une certaine importance, s'agissant des conséquences attachées à l'inscription d'une personne dans un fichier d'antécédents, en ce sens que l'incommodité d'être fiché ne s'accompagne pas d'une impossibilité d'accès à certaines activités professionnelles [52]. L'inscription dans le fichier de police en cause n'est ni une punition ni une peine complémentaire, sa finalité est clairement circonscrite à l'enquête judiciaire et son utilisation est réservée à des services soumis à une obligation de confidentialité.

57. Il n'en demeure pas moins qu'il s'agit d'un fichier unique servant des buts de police judiciaire extrêmement vastes, contenant des informations diversifiées, allant des simples renseignements d'état civil aux données biométriques et génétiques, et recensant des individus ne relevant pas du même statut procédural. Plutôt qu'un seul et même traitement englobant l'ensemble des informations, il a été jugé préférable, dans d'autres réglementations, de prévoir une pluralité de fichiers de police poursuivant des finalités spécifiques, ayant une seule utilisation et enregistrant un type de données.

### *b) Sur les infractions et les personnes concernées*

58. La conservation des données dans le fichier de police concerne les personnes mises en examen et condamnées pour des infractions intentionnelles poursuivies d'office, en ce sens que l'accusation est engagée par le procureur. Selon les indications du gouvernement bulgare, sont exclus de cette catégorie les infractions non intentionnelles, les délits et les crimes de nature

[51] Arrêt du 22 novembre 2022, Luxembourg Business Registers (C-37/20 et C-601/20, EU:C:2022:912, point 66).

[52] De manière générale, la présence dans le fichier n'implique aucune obligation positive pour la personne concernée.

privée, ainsi que certaines infractions qui ont fait l'objet d'une sanction administrative. Il a déjà été relevé que la grande majorité des infractions prévues par le code pénal sont intentionnelles et presque toutes sont poursuivies d'office [53].

59. Force est de constater que la réglementation nationale ne vise pas des infractions limitativement énumérées, n'opère pas de distinction des infractions selon leur nature, elle-même liée à la gravité des faits et à la peine applicable, ni ne retient de critère tenant à un quantum précis d'une peine d'emprisonnement. Se trouvent donc regroupés dans un ensemble unique et large des comportements infractionnels variés avec, certes, une réserve liée à la nécessité de la faute intentionnelle, ce qui conduit a priori à l'exclusion des infractions de faible gravité pour lesquelles la simple commission matérielle des faits incriminés suffit [54] ainsi que les infractions caractérisées par une faute simple d'imprudence ou de négligence. Invité lors de l'audience à préciser la teneur de la catégorie d'infractions en cause, le gouvernement bulgare s'est malheureusement borné à indiquer qu'il ne s'agit pas seulement d'infractions passibles d'une peine d'emprisonnement de cinq ans au moins.

60. S'agissant des individus concernés, il convient d'observer que le traitement incriminé des données est limité eu égard à l'âge des personnes concernées, puisqu'il résulte de l'article 4 du NRISPR que les mineurs ne sont pas soumis à l'enregistrement au fichier de police, ce qui réduit d'autant le nombre de personnes inscrites dans ce fichier. La mesure en cause distingue deux catégories d'individus, à savoir les personnes mises en examen et celles condamnées pénalement. Les personnes ainsi visées ont été préalablement identifiées, dans le cadre des procédures nationales applicables et sur la base d'éléments objectifs et non discriminatoires, comme présentant une menace pour la sécurité publique ou le maintien de l'ordre public. Les États membres ont la faculté de prendre des mesures de conservation visant des personnes faisant, au titre d'une telle identification, l'objet d'une mise en examen, c'est-à-dire une catégorie de personnes pour lesquelles il existe des motifs sérieux de croire qu'elles ont commis une infraction pénale, ou d'une condamnation traduisant le fait que leur responsabilité pénale a été établie, situations pouvant impliquer un risque élevé de récidive [55]. La récidive, entendue dans le sens commun plus large d'une réitération infractionnelle, est un phénomène que chaque État membre tente de mesurer et dont il essaie de comprendre les déterminants, tâche délicate, car dépendant de la disponibilité de données statistiques objectives et fiables concernant la délinquance. Lorsqu'elles existent, elles peuvent révéler que le passé pénal est un déterminant important de la récidive [56].

[53] Arrêt du 26 janvier 2023, Ministerstvo na vatreshnite raboti (Enregistrement de données biométriques et génétiques par la police) (C-205/21, EU:C:2023:49, point 78).

[54] Infractions fréquentes dans le domaine de la délinquance routière.

[55] Voir, par analogie, arrêt du 5 avril 2022, Commissioner of An Garda Síochána e.a. (C-140/20, EU:C:2022:258, points 77 et 78). Je relève que, dans l'arrêt du 21 juin 2022, Ligue des droits humains (C-817/19, EU:C:2022:491, point 198), la Cour a considéré qu'il découle de la directive 2016/681 que les critères utilisés aux fins de l'évaluation préalable des passagers doivent être déterminés de manière à cibler, spécifiquement, les individus sur desquels pourrait peser un *soupçon raisonnable* de participation à des infractions terroristes ou à des formes graves de criminalité visées par cette directive.

[56] Selon le bulletin *Infostat Justice* du ministère de la Justice français, nº 183, du 2 juillet 2021, « Mesurer et comprendre les déterminants de la récidive des sortants de prison », 86 % des sortants de prison en 2016 avaient déjà une mention au casier judiciaire avant la condamnation à l'origine de leur détention. Le taux de récidive augmente avec le nombre de condamnations antérieures : seulement 14 % des sortants de détention qui n'avaient aucune condamnation dans les cinq années précédant celle qui les a menés en prison récidivent dans l'année, contre 23 % de ceux qui avaient une condamnation et 63 % de ceux qui avaient été condamnés au moins dix fois.

61. Il importe encore de souligner que les personnes mises en examen et leurs données sont appelées à « disparaître » du fichier de police lorsque la procédure pénale les concernant s'achève par une décision de classement ou d'acquittement selon les termes de l'article 68 du ZMVR, ce qui influe bien évidemment sur le nombre de personnes inscrites au fichier que le gouvernement bulgare n'a pas été en mesure de communiquer [57].

### *c) Sur la nature des données et la durée de conservation*

62. En ce qui concerne les données concernées, la Cour a jugé que, eu égard à la protection accrue des personnes à l'égard du traitement de données sensibles, il y a lieu, pour le responsable de ce traitement, de s'assurer que cet objectif ne peut pas être satisfait en ayant recours à des catégories de données autres que celles énumérées à l'article 10 de la directive 2016/680 [58]. Ainsi qu'il a été exposé, les données dont la conservation est prévue sont manifestement de nature à contribuer à la prévention, à la détection ou à la poursuite d'infractions relevant de la lutte contre la criminalité et le maintien de l'ordre public. De même, il me semble difficile de considérer que ces finalités puissent être satisfaites de manière aussi efficace uniquement à partir de renseignements d'état civil ou de clichés photographiques de l'individu concerné, sauf à limiter excessivement la capacité des enquêteurs à élucider les infractions sur la base d'une comparaison des données recueillies au cours de l'enquête avec celles enregistrées dans le fichier à l'occasion d'enquêtes précédentes [59]. Le temps est fort heureusement révolu où l'aveu était considéré comme la reine des preuves, les éléments recueillis par les services de police technique et scientifique ayant avantageusement remplacé dans la hiérarchie probatoire une preuve sujette à caution. Il est donc possible de conclure que les données concernées sont tout à la fois pertinentes et non excessives au regard des finalités assignées au traitement.

63. Il convient de relever, par ailleurs, l'absence dans la réglementation nationale en cause de fixation d'une durée maximum précise de conservation des informations enregistrées dans le fichier, les données étant conservées seulement le temps de la procédure, s'achevant par une décision de classement ou d'acquittement pour certaines personnes mises en examen ou leur vie durant pour les personnes finalement condamnées. Selon les indications fournies à l'audience par le gouvernement bulgare, qu'il appartiendra à la juridiction de vérifier, la suppression intervient d'office au décès de l'intéressé, les héritiers disposant, en outre, du droit de demander l'effacement de l'inscription selon l'article 68, paragraphe 6, du ZMVR. Faut-il considérer que cette situation correspond, en relation avec les termes de l'article 5 de la directive 2016/680, à l'absence de fixation de délais appropriés pour l'effacement des données personnelles, dans le sens où la notion de délai devrait nécessairement correspondre à une période exprimée en

[57] Cette constatation traduit, au demeurant, le respect par cette disposition de l'article 6 de la directive 2016/680 imposant au responsable du traitement, le cas échéant et dans la mesure du possible, d'opérer une distinction claire entre les données des différentes catégories de personnes concernées, de manière à ce que le même degré d'ingérence dans leur droit fondamental à la protection de leurs données à caractère personnel ne leur soit pas indifféremment imposé, quelle que soit la catégorie à laquelle elles appartiennent [arrêt du 26 janvier 2023, Ministerstvo na vatreshnite raboti (Enregistrement de données biométriques et génétiques par la police) (C-205/21, EU:C:2023:49, point 83].

[58] Arrêt du 26 janvier 2023, Ministerstvo na vatreshnite raboti (Enregistrement de données biométriques et génétiques par la police) (C-205/21, EU:C:2023:49, point 126).

[59] Voir, par analogie, arrêt du 26 janvier 2023, Ministerstvo na vatreshnite raboti (Enregistrement de données biométriques et génétiques par la police) (C-205/21, EU:C:2023:49, point 100). Signalons également que l'écoulement du temps sera inévitablement un obstacle pour ce qui est de la localisation des témoins et de la capacité de ces derniers à bien se rappeler les événements.

années, mois ou jours ? Dans l'affirmative, cette même disposition impliquerait, à titre d'alternative, la fixation, dans la réglementation nationale, de délais pour la vérification périodique de la nécessité de conserver ces données [60].

64. S'agissant des données des personnes mises en examen et compte tenu du choix du législateur bulgare de ne pas les conserver en l'absence de condamnations pénales à l'issue de la procédure les concernant, la durée nécessairement aléatoire de cette dernière ne permet guère d'autres choix, sauf à formaliser un délai butoir pour prévenir une durée de procédure excessive. Quant aux personnes condamnées, je considère que la mention du décès est bien celle d'une limite temporelle, liée à la vie biologique de la personne concernée, excluant toute qualification de durée indéfinie ou illimitée pour la conservation des données [61]. L'expiration de la conservation est prédéterminée même si la date exacte de celle-ci est, par définition, indéterminée. En tout état de cause, je relève que le gouvernement bulgare a indiqué, lors de l'audience, qu'il existe une vérification périodique en interne des inscriptions au fichier, effectuée en l'occurrence tous les trois mois, ce qui satisfait aux exigences de l'article 5 de la directive 2016/680.

65. Reste qu'il est incontestable que, suivant l'âge auquel la personne concernée sera enregistrée dans le fichier et celui de son décès, la conservation pourra s'avérer très longue, d'une durée supérieure à celle prévue pour constater une récidive ou au délai de prescription de l'action publique pour l'infraction la plus grave [62]. Cette durée de conservation trouve néanmoins une justification dans la finalité de police judiciaire du traitement, celle de rassembler des indices et des preuves en vue d'identifier les auteurs d'infractions passées ou futures, étant observé que le risque afférent aux infractions pénales, qu'elles soient graves ou pas, présente un caractère général et permanent [63]. La résolution parfois très tardive d'affaires non élucidées montre tout à la fois la grande difficulté à laquelle se trouvent confrontés les services d'enquête et la pertinence de la conservation sur un long terme des données biométriques et génétiques recueillies dans les fichiers [64].

[60] L'article 31 du règlement (UE) 2016/794 du Parlement européen et du Conseil, du 11 mai 2016, relatif à l'Agence de l'Union européenne pour la coopération des services répressifs (Europol) et remplaçant et abrogeant les décisions du Conseil 2009/371/JAI, 2009/934/JAI, 2009/935/JAI, 2009/936/JAI et 2009/968/JAI (JO 2016, L 135, p. 53) prévoit que les données à caractère personnel traitées par Europol ne sont conservées par celle-ci que pour la durée nécessaire et proportionnée aux finalités pour lesquelles ces données sont traitées. Europol réexamine, en toute hypothèse, la nécessité de continuer à conserver ces données au plus tard trois ans après le début de leur traitement initial et peut décider de les conserver jusqu'à l'examen suivant, qui a lieu à l'issue d'une nouvelle période de trois ans, si leur conservation reste nécessaire pour lui permettre de remplir ses missions. En l'absence de décision de conserver plus longtemps des données à caractère personnel, celles-ci sont effacées automatiquement après trois ans.

[61] Dans l'arrêt du 13 février 2020, Gaughran c. Royaume-Uni (CE:ECHR:2020:0213JUD004524515, §§ 79 à 81), concernant une réglementation prévoyant une conservation des données prenant fin au décès de l'intéressé, une distinction a été établie entre, d'une part, l'ADN et, d'autre part, les empreintes ainsi que les photographies. La Cour EDH a considéré que seules les dernières données faisaient l'objet d'une période de conservation assimilable à une conservation à durée indéfinie. Je relève, pour ma part, qu'aucune de ces données ne pourra, en l'occurrence, être utilisée une fois survenu le décès de la personne concernée, étant observé que la conservation post mortem de l'ADN aurait rendu techniquement possible une recherche auprès des proches parents de l'intéressé.

[62] Outre l'existence d'infractions imprescriptibles, la question de la relation du délai de conservation des données à celui de la prescription de l'action publique doit être relativisée, dans certains systèmes juridiques, du fait des mécanismes de suspension ou d'interruption de la prescription et du report du point de départ du délai de prescription pour les infractions dites d'habitude, continues ou dissimulées ainsi que pour certaines infractions dont sont victimes les mineurs (report à la majorité de la victime). Il convient également de prendre en compte le fait que les violences sexuelles sont celles qui sont révélées le plus tardivement.

[63] Voir, en ce sens, arrêt du 5 avril 2022, Commissioner of An Garda Síochána e.a. (C-140/20, EU:C:2022:258, point 62).

[64] Je rappelle que la Cour EDH a, dans le contexte de l'obligation positive découlant de l'article 2 de la CEDH, fermement reconnu l'intérêt public à enquêter et éventuellement à obtenir la poursuite et la condamnation des auteurs d'actes illicites, plusieurs années après les faits (Cour EDH, 12 juin 2014, Jelić c. Croatie, CE:ECHR:2014:0612JUD005785611, § 52), et indiqué que l'enquête sur les « cold cases » relève également de l'intérêt public, au sens général de la lutte contre la criminalité (Cour EDH, 13 février 2020, Gaughran c. Royaume-Uni, CE:ECHR:2020:0213JUD004524515, § 93).

### *d) Sur l'existence de garanties juridiques et techniques en matière de conservation et d'accès aux données*

66. La proportionnalité de l'ingérence qu'implique la conservation des données se trouvant dans le fichier de police ne peut pas être examinée indépendamment des règles régissant l'accès à ce fichier et le contrôle de la justification du maintien des données dans ce dernier. Selon la Cour EDH, lorsqu'un État s'attribue le pouvoir le plus large de conservation à durée indéterminée, l'existence et le fonctionnement de certaines garanties effectives deviennent déterminants. Ainsi, le droit interne doit contenir des garanties de nature à protéger efficacement les données à caractère personnel enregistrées contre les usages impropres et abusifs et permettre la suppression de ces données dès lors que leur conservation continue devient disproportionnée, notamment en offrant une possibilité concrète de présenter une requête en effacement des données mémorisées [65].

#### *1) Sur les conditions de consultation du fichier*

67. Il ressort des considérants 28, 56 et 57 de la directive 2016/680 ainsi que de ses articles 24, 25 et 29 que les États membres doivent prendre des mesures visant à ce que les données personnelles soient traitées de manière à garantir un niveau de sécurité et de confidentialité approprié, notamment en empêchant l'accès non autorisé à ces données et à l'équipement assurant leur traitement de même que l'utilisation non autorisée de ces données et de cet équipement. Ces mesures comprennent la tenue, par le responsable du traitement, de registres à même de fournir à l'autorité de contrôle, à sa demande, un certain nombre d'informations sur le traitement des données effectuées ainsi que des journaux pour certaines opérations de traitement telles que la consultation, les transferts et l'effacement. Selon le considérant 60 de la directive 2016/680, le responsable du traitement doit mettre en œuvre des mesures pour atténuer les risques, précédemment évalués, inhérents au traitement concerné, ces risques tenant, notamment, à la divulgation ainsi qu'à l'accès non autorisés de données.

68. Lors de l'audience, le gouvernement bulgare a fait état du respect de ces exigences par la réglementation nationale, évoquant l'existence d'un corps de règles prévoyant, notamment, l'établissement de listes nominatives d'agents ayant accès aux données, la nécessité pour chaque usager d'indiquer la justification de son droit d'accès, son identité, la date et l'heure de l'accès [66]. Ces garanties quant au champ des personnes habilitées à consulter le fichier et aux modalités de consultation de ce dernier apparaissent de nature à prévenir toute utilisation abusive ou frauduleuse d'un accès aux fichiers et par là même une atteinte excessive aux droits fondamentaux consacrés aux articles 7 et 8 de la Charte, ce qu'il appartiendra à la juridiction de renvoi de vérifier.

#### *2) Sur le contrôle du maintien des données dans le fichier*

69. Il est constant que le contrôle susmentionné, tel que prévu à l'article 68, paragraphe 6, du ZMVR, est de nature duale puisque s'effectuant d'office par les autorités compétentes, sous la forme d'un autocontrôle, et sur demande motivée de l'intéressé ou de ses héritiers, les motifs de radiation d'une inscription dans le fichier étant, dans les deux cas de figure, énoncés de manière exhaustive dans cette disposition. Ces motifs ne comprennent pas la situation d'un individu

[65] Cour EDH, 22 juin 2017, Aycaguer c. France (CE:ECHR:2017:0622JUD000880612, § 38), et Cour EDH, 13 février 2020, Gaughran c. Royaume-Uni (CE:ECHR:2020:0213JUD004524515, § 88).

[66] La durée de conservation des traces de consultation du fichier n'a pas été précisée.

ayant fait l'objet d'une réhabilitation, entraînant l'effacement de la condamnation concernée de son casier judiciaire, et seul le motif visé à l'article 68, paragraphe 6, point 1, du ZMVR, concernant un enregistrement effectué en violation de la loi, est susceptible de fonder la requête en effacement d'une personne condamnée pénalement présentée, comme en l'espèce, de son vivant et donc avant expiration de la durée légale de conservation fixée au décès de celle-ci.

70. Interrogé lors de l'audience sur la portée de l'article 68, paragraphe 6, du ZMVR, eu égard à l'application qui en est faite par les autorités et les juridictions compétentes, le gouvernement bulgare a précisé que cette disposition permettait de modifier une inscription concernant une personne mise en examen devenue incorrecte à la suite d'une requalification de l'infraction par le tribunal. Il a exclu toute possibilité d'effacement d'une inscription dans le fichier à la suite d'une réhabilitation de la personne condamnée. Je rappelle, à cet égard, que le fichier en cause constitue un outil d'investigation visant à faciliter l'activité opérationnelle de police judiciaire et non, à proprement parler, un fichier d'antécédents pénaux comme le casier judiciaire. Ces deux instruments ne répondent pas à la même finalité : l'un est une mémoire au service exclusif des enquêteurs pour leur permettre, sur le long terme, d'élucider des infractions passées ou futures, l'autre a pour vocation de guider le travail des juges lors du prononcé de la sanction pénale dans une affaire donnée. Ainsi, au bénéfice de la réhabilitation ayant entraîné l'effacement de la condamnation concernée du casier judiciaire, l'individu pourrait se retrouver, le cas échéant, dans la situation d'un primo-délinquant, susceptible de bénéficier de peines plus légères ou d'aménagements de peine. Pour autant, la conservation de ses données dans le fichier demeure en principe nécessaire au regard de l'objectif plus large de ce dernier relatif à la détection, l'élucidation et la prévention des infractions.

71. Reste qu'il ressort des observations du gouvernement bulgare que le motif visé à l'article 68, paragraphe 6, point 1, du ZMVR ne recouvre pas une appréciation de la nécessité de la conservation des données dans sa dimension temporelle. Il semble qu'il n'existe aucune disposition dans la réglementation nationale, pas plus qu'une pratique administrative ou juridictionnelle, qui permettent à l'autorité compétente de radier, dans le cadre des vérifications trimestrielles, l'inscription au fichier ou à l'individu concerné de demander l'effacement de celle-ci si la conservation des données personnelles n'apparaît plus nécessaire compte tenu du temps écoulé depuis l'enregistrement. La juridiction de renvoi appelée à connaître de la légalité de la décision de rejet de la demande d'effacement ne paraît pas davantage être en capacité d'effectuer une telle appréciation.

## F. Conclusion intermédiaire

72. Peut-on considérer que les critères utilisés aux fins de la conservation des données, décrits ci-dessus, présentent un caractère suffisamment ciblé, proportionné et spécifique et que le traitement des données personnelles en cause respecte les limites du strict nécessaire ou de l'absolue nécessité ? La Cour pourrait donner une réponse négative à cette interrogation pour les motifs suivants.

73. Il importe de souligner, en premier lieu, que la problématique de la nécessité de la conservation des données personnelles se pose avec une particulière acuité lorsque le traitement de ces dernières est autorisé, comme en l'espèce, à des fins préventives. À cet égard, le véritable critère justifiant l'enregistrement et la conservation des données dans le fichier de police en cause est la dangerosité que présentent les personnes concernées, ce qui implique une évaluation des risques. Dans le cas présent, force est de constater que cette évaluation s'arrête au seul constat de l'existence d'une suspicion ou de la commission avérée d'une infraction intentionnelle, critère peu

spécifique s'il en est, s'agissant d'un élément constitutif des infractions, voire du fondement même de la responsabilité pénale. Ainsi, le régime national de conservation me paraît tenir compte d'un degré de gravité minimal par rapport à l'infraction et recouvre une grande diversité d'atteintes à l'ordre social, sans que soit a priori requise une sanction constituée par une peine d'emprisonnement, ce qui permet de considérer qu'il s'applique quelle que soit la nature ou la gravité de l'infraction [67]. Je rappelle que la Cour a considéré que la législation bulgare, telle que celle en cause dans le litige au principal, qui prévoit la collecte des données biométriques et génétiques de toute personne mise en examen pour une infraction intentionnelle poursuivie d'office, est, en principe, contraire à l'exigence énoncée à l'article 10 de la directive 2016/680, car elle est susceptible de conduire, de manière indifférenciée et généralisée, à cette collecte, dès lors que la notion d'« infraction pénale intentionnelle poursuivie d'office » revêt un caractère particulièrement général et est susceptible de s'appliquer à un grand nombre d'infractions pénales, indépendamment de leur nature et de leur gravité [68].

74. Si des études statistiques peuvent révéler que le passé pénal est un déterminant important de la récidive, elles soulignent aussi l'existence de facteurs objectifs aggravant le risque de récidive liés, notamment, au genre, à l'âge et à la nature de l'infraction initiale, de délais de réitération du comportement infractionnel et du fait que l'infraction en récidive est très liée à la nature de l'infraction à l'origine de la détention [69]. Or, en retenant comme critère de conservation des données jusqu'au décès de l'intéressé toute condamnation pour une infraction intentionnelle, y compris la première [70], il apparaît que la logique sous-jacente du traitement de ces données est celle d'une appréhension particulièrement extensive du parcours de délinquance, qu'il s'agisse tant de la nature et/ou de la gravité des actes délictueux que de l'âge du contrevenant. À l'instar de la Cour EDH, on peut se demander si, poussé d'une certaine manière à l'extrême, ce type de logique ne revient pas en pratique à justifier le stockage d'informations sur l'ensemble de la population et sur leurs parents décédés, ce qui serait assurément excessif et dénué de pertinence [71]. Je note que la Cour a considéré que le seul fait qu'une personne soit mise en examen pour une infraction pénale intentionnelle poursuivie d'office ne saurait être considéré comme un élément permettant, à lui seul, de présumer que la collecte de ses données biométriques et génétiques est absolument nécessaire au regard des finalités qu'elle vise [72].

75. Il apparaît, en second lieu, que les données sont conservées sans égard à la nécessité de mémoriser celles-ci jusqu'au décès de la personne concernée. Compte tenu du libellé de l'article 68, paragraphe 6, du ZMVR et de l'interprétation qui en est faite, les autorités compétentes ne sont investies du pouvoir d'effacer les données que dans des circonstances exceptionnelles, sans rapport avec l'évolution de la situation de cette personne depuis

67 Cour EDH, 13 février 2020, Gaughran c. Royaume-Uni (CE:ECHR:2020:0213JUD004524515, § 83).

68 Arrêt du 26 janvier 2023, Ministerstvo na vatreshnite raboti (Enregistrement de données biométriques et génétiques par la police) (C-205/21, EU:C:2023:49, points 128 et 129).

69 Bulletin *Infostat Justice* du ministère de la justice français, n° 183, du 2 juillet 2021, « Mesurer et comprendre les déterminants de la récidive des sortants de prison ».

70 L'enregistrement et la conservation subséquente des données dans le fichier concernent, en effet, tout primo-délinquant et non un individu déjà condamné à une ou plusieurs reprises.

71 Cour EDH, 13 février 2020, Gaughran c. Royaume-Uni (CE:ECHR:2020:0213JUD004524515, § 89).

72 Arrêt du 26 janvier 2023, Ministerstvo na vatreshnite raboti (Enregistrement de données biométriques et génétiques par la police) (C-205/21, EU:C:2023:49, point 130). La Cour ajoute (points 132 et 133) qu'il appartient à la juridiction de renvoi de vérifier si le droit national permet d'apprécier la « nécessité absolue » de procéder à la collecte des données biométriques et génétiques de la personne concernée aux fins de leur enregistrement eu égard à la nature et la gravité de l'infraction dont cette personne est suspectée mais aussi à d'autres éléments pertinents tels que, notamment, les circonstances particulières de cette infraction, le lien éventuel de ladite infraction avec d'autres procédures en cours, les antécédents judiciaires ou le profil individuel de la personne en cause. On peut se demander si cette exigence d'individualisation approfondie est compatible avec des dispositions de nature législative, avec le caractère systématique et le degré d'abstraction et de généralité qu'elles requièrent, visant à établir un régime général de conservation des données personnelles dans un fichier.

l'enregistrement dans le fichier. Il en va logiquement de même du recours en effacement, prévu par le même texte, dont dispose ladite personne, lequel ne présente pas un caractère d'effectivité suffisant comme ne permettant pas de vérifier que la durée de conservation des données soit proportionnée au but de l'ingérence en cause. Cette appréciation devrait tenir compte de différents critères, tels que la nature et la gravité des faits constatés, le temps écoulé depuis les faits, la durée légale de conservation restant à courir ou l'âge du requérant en l'espèce, et ce au regard de sa situation personnelle, s'agissant de l'âge auquel celui-ci a commis les faits, de son comportement depuis (insertion sociale, dédommagement des victimes), de sa personnalité, le bénéfice d'une réhabilitation pouvant, dans ce contexte, constituer un élément de l'appréciation d'ensemble. Dans ces circonstances, le contrôle dont dispose, notamment, la personne inscrite au fichier apparaît tellement étroit qu'il est quasi hypothétique [73].

76. Les constatations opérées ci-dessus doivent être rapprochées du fait que peuvent être conservées sur un très long terme des données sensibles et que le fichier en cause est à même d'offrir à ses utilisateurs des fonctionnalités d'exploitation de celles-ci, notamment d'identification, d'analyse et de rapprochement, très intrusives. Il convient de relever que, conformément à l'article 68, paragraphe 3, du ZMVR, les autorités de police doivent, pour les besoins de l'inscription dans le fichier de police, effectuer des prélèvements aux fins du « profilage ADN » des personnes et photographier celles-ci, clichés pouvant, le cas échéant, se voir appliquer la technique de reconnaissance faciale.

## V. Conclusion

77. À la lumière des considérations qui précèdent, je propose à la Cour de répondre comme suit au Varhoven administrativen sad (Cour administrative suprême, Bulgarie) :

Les articles 4, 5, 8, 10 et l'article 16, paragraphe 2, de la directive (UE) 2016/680 du Parlement européen et du Conseil, du 27 avril 2016, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil, lus de manière combinée et à la lumière de l'article 52, paragraphe 1, de la charte des droits fondamentaux de l'Union européenne,

doivent être interprétés en ce sens que :

ils s'opposent à une législation nationale prévoyant la conservation de données à caractère personnel dans un fichier de police, incluant les données biométriques et génétiques, de toute personne condamnée pénalement pour une infraction intentionnelle, sans autre différenciation quant à la nature ou la gravité de l'infraction, et ce jusqu'au décès de celle-ci, sans possibilité d'un contrôle du maintien des données y figurant au regard du temps écoulé depuis leur enregistrement et, le cas échéant, de l'obtention subséquente de l'effacement de celles-ci.

La vérification de la proportionnalité de la durée de conservation des données à la finalité du traitement au regard de la situation de la personne condamnée peut inclure la réhabilitation dont cette dernière a fait l'objet.

[73] Cour EDH, 13 février 2020, Gaughran c. Royaume-Uni (CE:ECHR:2020:0213JUD004524515, § 94).