ORGANE DE CONTRÔLE DE L'INFORMATION POLICIÈRE

Votre référence	Notre référence	Annexe(s)	Date
	DA230032		05.09.2023

<u>Objet :</u> Avis relatif à l'avant-projet de loi portant dispositions en matière de digitalisation de la justice et dispositions diverses

L'Organe de contrôle de l'information policière (ci-après le 'COC' ou 'l'Organe de contrôle').

Vu la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel (M.B. du 5 septembre 2018, ci-après 'la LPD'), en particulier l'article 59 §1er, 2e alinéa, l'article 71 et le Titre VII, en particulier l'article 236.

Vu la loi du 3 décembre 2017 portant création de l'Autorité de protection des données (ci-après 'la LAPD').

Vu la loi du 5 août 1992 sur la fonction de police (ci-après 'la LFP').

Vu la *Law Enforcement Directive* 2016/680 du 27 avril 2016 (ci-après 'la *LED*').

Vu la loi du 25 décembre 2016 relative au traitement des données des passagers.

Vu la demande adressée le 20 juillet 2023 par le Vice-premier ministre et ministre de la Justice à l'Organe de contrôle.

Vu la transmission en date du 02 août 2023, par l'Autorité de protection des données (ci-après 'l'APD'), de la demande susmentionnée à l'Organe de contrôle dans le cadre du principe du guichet unique (cf. art. 54/1 §1er de la LAPD).

Vu le rapport de Monsieur Frank Schuermans, président *a.i.* de l'Organe de contrôle.

Émet, le 5 septembre 2023, l'avis suivant.

I. Remarque préalable concernant la compétence de l'Organe de contrôle

1. À la lumière respectivement de l'application et de la transposition du Règlement 2016/679[1] et de la Directive 2016/680[2], le législateur a remanié en profondeur les tâches et missions de l'Organe de contrôle. L'article 4 §2, quatrième alinéa de la loi du 3 décembre 2017 portant création de l'Autorité de protection des données (ci-après 'la LAPD') dispose qu'à l'égard des services de police au sens de l'article 2, 2°, de la loi du 7 décembre 1998 organisant un service de police intégré, structuré à deux niveaux, les compétences, missions et pouvoirs d'autorité de contrôle tels que prévus par le Règlement 2016/679 sont exercés par l'Organe de contrôle. Cela signifie notamment que l'Organe de contrôle est compétent également lorsque des services de police traitent des données à caractère personnel qui ne relèvent pas des missions de police administrative et judiciaire, par exemple dans le cadre de finalités socioéconomiques ou de traitements relevant de la gestion des ressources humaines. L'Organe de contrôle doit être consulté lors de la préparation de la législation ou d'une mesure réglementaire ayant trait au traitement de données à caractère personnel par les services de police de la police intégrée (voir les articles 59 §1er, 2e alinéa et 236 §2 de la LPD, l'article 36.4 du RGPD et l'article 28.2 de la directive Police-Justice). L'Organe de contrôle a dans ce contexte pour mission d'examiner si l'activité de traitement projetée par les services de police est conforme aux dispositions du Titre 1er (pour les traitements non opérationnels)[3] et du Titre 2 (pour les traitements opérationnels) de la LPD[4]. De plus, le COC est aussi chargé d'émettre des avis d'initiative, comme prévu à l'article 236 §2 de la LPD, et est investi conformément à l'article 240 de la LPD d'une mission générale d'information à l'égard du grand public, des personnes concernées, des responsables du traitement et des sous-traitants dans le domaine du droit à la protection des données et à la protection de la vie privée.

2. En ce qui concerne en particulier les activités de traitement dans le cadre des missions de police administrative et/ou judiciaire, l'Organe de contrôle émet dès lors des avis soit d'initiative, soit à la demande du Gouvernement ou de la Chambre des Représentants, d'une autorité administrative ou judiciaire ou d'un service de police, concernant toute matière ayant trait à la gestion de l'information policière telle que régie par la Section 12 du Chapitre 4 de la loi sur la fonction de police[5].

---

[1] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 *« relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE »* (règlement général sur la protection des données ou « RGPD »).

[2] 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 »* (ci-après dénommée « directive Police-Justice » ou *Law Enforcement Directive* (*LED*)).

[3] Article 4 §2, 4e alinéa de la LPD.

[4] Article 71 §1er, 3e alinéa de la LPD.

[5] Articles 59 §1er, 2e alinéa et 236 §2 de la LPD.

3. Par ailleurs, l'Organe de contrôle est également chargé, à l'égard des services de police, de l'inspection générale de la police fédérale et de la police locale (en abrégé 'AIG') visée dans la loi du 15 mai 2007 sur l'Inspection générale et de l'Unité d'information des passagers (ci-après dénommée en abrégé 'BELPIU') visée au Chapitre 7 de la loi du 25 décembre 2016, de la surveillance de l'application du Titre 2 de la LPD et/ou du traitement de données à caractère personnel tel que visé aux articles 44/1 à 44/11/13 de la loi sur la fonction de police, et/ou de toute autre mission qui lui est confiée en vertu ou par d'autres lois[6].

4. L'Organe de contrôle est compétent à l'égard du Service Contentieux de l'Administration générale des Douanes et Accises en ce qui concerne les réquisitions adressées par ce service à la BELPIU dans des matières fiscales, et ce en vertu de l'article 281 §4 de la loi générale *« sur les douanes et accises »* du 18 juillet 1977, telle que modifiée par la loi du 2 mai 2019 *« modifiant diverses dispositions relatives au traitement des données des passagers »*.

5. Enfin, l'Organe de contrôle est également chargé, dans le cadre de la législation sur la rétention des données et en vertu de l'article 126/3 §1er, 8e alinéa de la loi du 13 juin 2005 relative aux communications électroniques (ci-après 'la LCE'), telle que modifiée par la loi du 20 juillet 2022 relative à la collecte et à la conservation des données d'identification et des métadonnées dans le secteur des communications électroniques et à la fourniture de ces données aux autorités (*M.B.* du 8 août 2022), de la validation des statistiques relatives au nombre de faits punissables et au délai de conservation pour chaque arrondissement judiciaire et chaque zone de police, une matière dans le cadre de laquelle il exerce toutes les compétences qui lui ont été attribuées par le Titre 7 de la loi du 30 juillet 2018. Il est par ailleurs également chargé, en application de l'article 42 §3, 2e et 3e alinéas de la LFP, du contrôle des requêtes de la Cellule Personnes disparues de la police fédérale en vue de la consultation des données relatives aux communications électroniques impliquant la personne disparue.

6. L'Organe de contrôle est compétent pour rendre des avis sur les aspects ayant trait au traitement des informations et des données à caractère personnel et à la protection de la vie privée par le traitement de données à caractère personnel pour autant qu'il existe un rapport avec le fonctionnement opérationnel et non opérationnel des services de police et/ou avec le personnel de la police intégrée (ci-après 'la GPI[7]') et/ou pour autant que le projet de texte soumis pour avis ait un impact sur la gestion de l'information policière en général.

7. Par ailleurs, l'Organe de contrôle n'est pas seulement une autorité de protection des données, mais est aussi une autorité de contrôle qui est légalement chargée de contrôler la légalité, l'efficacité, l'efficience et l'économie de la gestion de l'information policière[8].

---

[6] Article 71 §1er, troisième alinéa *juncto* article 236 §3 de la LPD.
[7] Geïntegreerde politie – Police Intégrée.
[8] Rapport d'activité 2021, www.organedecontrole.be, voir les points 3 et 52 et plus spécifiquement le point 71 : *« Il serait cependant faux de s'imaginer que le COC se préoccupe seulement de la protection des données ; il porte aussi énormément*

I. Objet de la demande

8. La demande d'avis a trait à l'avant-projet de loi *« portant dispositions en matière de digitalisation de la justice et dispositions diverses »* (ci-après 'l'avant-projet'). La même demande a par la suite encore été transmise à l'Organe de contrôle par l'Autorité de protection des données (ci-après 'l'APD') dans le cadre du principe du guichet unique.

9. L'avant-projet prend un certain nombre de mesures diverses visant à digitaliser la justice à travers notamment la création d'un Registre central des dossiers pénaux et d'un système de gestion des dossiers, tout en réglementant notamment l'échange d'informations entre la police et la justice. En marge de ces mesures, l'avant-projet prévoit aussi une transposition partielle de la directive 2016/680 (ci-après 'la *LED*'), plus précisément en ce qui concerne l'exercice des droits liés à la protection des données de la personne concernée dans le cadre du droit de la procédure pénale.

10. Étant donné que l'avant-projet a un impact sur la gestion de l'information par la GPI, l'Organe de contrôle se limitera dans le présent avis aux aspects de l'avant-projet ayant trait à cette matière. En l'occurrence, cela signifie que le présent avis analysera les articles 21, 35 et 70 à 83 inclus de l'avant-projet. Pour le reste, l'Organe de contrôle renvoie à l'avis de l'APD.

II. Analyse de la demande

1. Remarque générale concernant la modification du Code d'instruction criminelle en rapport avec la *LED* (telle que transposée au Titre 2 de la LPD)

11. Bien que la formulation d'un avis concernant les modifications du Code d'instruction criminelle relève en l'occurrence en principe de la compétence de l'APD, le COC se voit dans l'obligation d'émettre quelques remarques générales concernant l'interprétation donnée dans l'exposé général par l'auteur de l'avant-projet à la portée de la *LED* et à sa prétendue *« contradiction fondamentale »* avec le droit de la procédure pénale. L'interprétation avancée par l'auteur de l'avant-projet, que nous aborderons ci-après, est en effet susceptible d'avoir un impact (négatif) sur l'application des droits de la personne concernée dans le cadre des traitements effectués par la police, une matière à l'égard de laquelle l'Organe de contrôle dispose de la plénitude de compétence.

12. Pour commencer, le COC tient à souligner qu'il apprécie la volonté de l'auteur de l'avant-projet de tenter de mettre en œuvre dans le cadre du droit de la procédure pénale (du moins en théorie) les

d'attention à tous les autres aspects opérationnels de la gestion de l'information policière et des informations des autres services qu'il contrôle, s'agissant là de matières relevant également de sa compétence. » ; article 71 §1er de la LPD.

droits fondamentaux de la personne concernée en matière de droit à la protection des données, et plus particulièrement les 'droits Franchimont'.

Une première question à se poser est toutefois de savoir si les textes en projet du Code d'instruction criminelle n'en deviennent pas encore bien plus complexes et plus ardus qu'ils ne le sont déjà. Le COC ne peut en effet que constater que depuis l'entrée en vigueur de la LPD le 5 septembre 2018 – c'est-à-dire en 5 ans –, il semble ne pas y avoir eu dans la pratique de problèmes (fondamentaux) dans le cadre d'une part de l'application des règles relevant purement de la procédure pénale régissant les 'droits Franchimont', et d'autre part de l'exercice des droits liés à la protection des données dans le contexte de l'enquête de police et/ou de l'enquête en matière pénale. Le COC n'a en tout cas pas connaissance de problèmes (pratiques) concrets, de jurisprudence problématique ni d'un quelconque signal négatif en la matière qui nécessiteraient de procéder à présent – 5 ans après l'entrée en vigueur de la *LED* et de la LPD – à cette intervention législative projetée. L'exposé des motifs, d'ailleurs, ne dit mot à ce sujet et ne fournit ni explications ni exemples motivant la nécessité de légiférer à présent.

Le COC ne cache pas ses doutes quant à la mise en œuvre concrète des nouveaux 'droits Franchimont' introduits par cet avant-projet en termes de complexité et de faisabilité, non seulement pour les professionnels du droit, mais à plus forte raison pour le citoyen. En conséquence, il appartient à l'auteur de l'avant-projet de réfléchir à l'opportunité de cette initiative.

Quoi qu'il en soit, comme le fait remarquer à juste titre l'auteur de l'avant-projet, la mise en œuvre concrète des droits spécifiques liés à la protection des données dans le contexte de l'information ou de l'instruction en matière pénale est un exercice très difficile[9]. **Néanmoins, le COC se pose des questions fondamentales quant à l'angle d'incidence et aux principes adoptés par l'auteur de l'avant-projet dans l'exposé des motifs.**

13. En ce qui concerne les lignes de force (du Titre 2) de la LPD, l'auteur de l'avant-projet adopte aux pages 22 et 23 de l'exposé des motifs un point de vue qui est déterminant pour l'intégration des droits de la personne concernée dans les dispositions en projet des 'droits Franchimont' (citation littérale) : *« La loi sur la protection des données contient plusieurs directives relatives à l'exercice des droits liés à la protection de la vie privée qui déterminent l'option choisie et consistent à intégrer l'exercice de ces droits dans le Code d'instruction criminelle. Il s'agit de la seule façon d'effectuer l'exercice extrêmement difficile qui consiste à trouver une solution à la contradiction fondamentale entre les points de départ du droit de la procédure pénale d'une part et de la protection des données d'autre part. »*[10].

[9] Exposé des motifs, p. 22.
[10] Soulignement du COC.

14. De l'avis du COC, les cadres juridiques du droit à la protection des données et les dispositions du droit de la procédure pénale poursuivent en effet deux objectifs différents, mais ne sont **pas** pour autant fondamentalement contradictoires. Le fait que les objectifs soient différents est logique et peut déjà être déduit de la Charte des droits fondamentaux de l'Union européenne (ci-après 'la Charte'). Quant à la *LED*, elle concrétise l'article 8 de la Charte[11], lequel garantit la protection des données à caractère personnel (ainsi que l'article 8 de la Convention européenne des droits de l'homme[12]). En revanche, les 'droits Franchimont' sont dans le droit de l'Union basés sur les droits énoncés aux articles 47 et 48 de la Charte (et à l'article 6 de la Convention européenne des droits de l'homme), dont la protection des droits des suspects ou prévenus dans le cadre d'une procédure pénale (e.a. l'accès au dossier pénal), la présomption d'innocence et les droits de la défense – bref, le droit à un procès équitable.

15. Les objectifs du droit à la protection des données poursuivent par contre d'**autres** objectifs, à savoir garantir grâce à l'harmonisation un niveau de protection élevé des droits et des intérêts des personnes dont les données à caractère personnel sont traitées, tandis que la *LED* aspire à la libre circulation des données à caractère personnel à la lumière de la finalité poursuivie par la *LED*. Pour cette raison, la personne concernée dispose conformément à l'article 8.2 de la Charte d'un certain nombre de droits fondamentaux ou, si l'on veut, de « droits de contrôle » à l'égard du traitement de ses données à caractère personnel. Ces droits de contrôle ont un but : ils visent à pouvoir contrôler la légitimité, à savoir la licéité du traitement, sa nécessité, sa proportionnalité, la qualité des données à caractère personnel, le délai de conservation et la sécurité (confidentialité et intégrité) des données à caractère personnel qui sont traitées. C'est pour cette raison que le responsable du traitement a en principe également à l'égard de la personne concernée un devoir d'information (qui concrétise le principe de transparence en tant que droit fondamental du droit à la protection des données). Cependant, à l'instar du droit à la protection de la vie privée, le droit fondamental à la protection des données à caractère personnel n'est pas absolu. Des restrictions des droits de contrôle peuvent être imposées pour autant que ce soit strictement nécessaire et que ce soit par ailleurs proportionnel à la finalité légale poursuivie par le traitement des données à caractère personnel (article 52 de la Charte, article 8.2 de la Convention européenne des droits de l'homme).

16. L'objectif (du discours) du droit à la protection des données (en l'occurrence la *LED*, et donc sa transposition au Titre 2 de la LPD) implique toutefois que, comme le fait à juste titre remarquer l'auteur

[11] Article 16 du Traité sur le fonctionnement de l'Union européenne (TFUE).
[12] Sachant que la Cour européenne des droits de l'homme répète par défaut que la protection des données à caractère personnel est d'une importance fondamentale pour la jouissance du droit à la protection de la vie privée. Bien que la Convention européenne des droits de l'homme ne prévoie pas de droit fondamental distinct à la protection des données à caractère personnel, la Cour européenne des droits de l'homme estime donc que la protection des données à caractère personnel découle de l'article 8 de la Convention européenne des droits de l'homme, mais y voit aussi un droit fondamental relevant du droit général « au respect de la vie privée » énoncé à l'article 8 de la Convention européenne des droits de l'homme étant donné qu'elle répète invariablement que la protection offerte par l'article 8 de la Convention européenne des droits de l'homme vaut indépendamment de la sensibilité des données à caractère personnel en termes de vie privée. La Cour européenne des droits de l'homme associe le lien avec la protection prévue par l'article 8 de la Convention européenne des droits de l'homme à la notion de « traitements ».

de l'avant-projet, la personne concernée peut uniquement exercer les droits de contrôle sur les données à caractère personnel **la concernant**, et donc **pas** sur les données à caractère personnel de **tiers**. De plus, le droit à la protection des données porte en principe uniquement sur les 'données à caractère personnel' et non sur les 'documents' ou 'pièces'. Néanmoins, un exercice adéquat du droit d'accès (droit fondamental) peut impliquer que dans les circonstances concrètes données (et donc au cas par cas), la personne concernée se voie remettre une copie (de la partie) du document dans lequel/de la pièce dans laquelle ses données à caractère personnel ont été traitées, dans laquelle les données de tiers auront le cas échéant été masquées[13]. Il convient toutefois de garder à l'esprit que contrairement au RGPD, la *LED* ne prévoit **pas** le droit à une copie, mais laisse aux États membres la liberté de prévoir cette possibilité[14]. Assez logiquement, l'article 38 de la LPD ne réglemente pas le droit à une copie.
Par ailleurs, l'exercice des droits de contrôle n'est pas non plus l'instrument de droit adéquat lorsque la personne concernée n'est pas d'accord avec les opinions (subjectives) et/ou points de vue et/ou constatations qu'un document ou une pièce donné(e) contient ou pourrait contenir dans le contexte de l'information ou de l'instruction en matière pénale. Autrement dit, les droits de contrôle ne visent pas le droit de « rectifier » ou d'« effacer » une certaine constatation, un certain point de vue ou une certaine opinion avec lequel (laquelle) la personne concernée n'est (dans les faits) pas d'accord, ni à faire « effacer » un élément de preuve en tant que tel.

17. À cet égard, le régime prévu pour les 'droits Franchimont' (comme faisant partie des droits énoncés aux articles 47 et 48 de la Charte) est d'une manière générale plus large, en ce sens que l'accès au dossier pénal ne se limite en principe pas aux données à caractère personnel du demandeur *« le concernant »*, mais porte aussi sur celles de tiers et sur les pièces du dossier pénal, même si celles-ci ne contiennent pas de données à caractère personnel référant directement ou indirectement au demandeur. Le droit à la protection des données ne confère ainsi pas à la personne concernée de droit d'accès à une analyse purement juridique[15], alors qu'une telle pièce peut faire partie du dossier pénal. Ces objectifs ne relèvent pas de la portée des droits de contrôle de la *LED* et du RGPD (article 8 de la Charte).

18. En outre, les dispositions de la *LED* et du RGPD stipulent que la personne concernée ne doit **pas** motiver *pourquoi* elle exerce ses droits de contrôle. La personne concernée peut donc se borner à demander si le ministère public (MP) (ou la police) traite ses données à caractère personnel. Elle ne doit pas motiver pourquoi elle souhaite obtenir cette information. Le motif figure en effet dans la *LED* elle-même (et donc dans le Titre 2 de la LPD): pour pouvoir vérifier la licéité, la nécessité, la proportionnalité, etc.[16] Il est donc particulièrement douteux, pour ne pas dire contraire à la *LED*, de soumettre la requête de la personne concernée à de telles conditions. Des dispositions du style *« à*

[13] Voir CJUE 4 mai 2023, C-487/21.
[14] Considérant 43, *in fine* de la *LED*.
[15] Cf. CJUE 17 juillet 2014, C-141/12 et C-372/12.
[16] Idem, avec référence à la jurisprudence antérieure.

peine d'irrecevabilité, la requête est motivée »[17] et *« si le requérant ne justifie pas d'un motif légitime la consultation du dossier »*[18], qui reviennent à dire que la personne concernée doit motiver son droit d'accès, semblent donc particulièrement problématiques.

19. Le COC comprend, et rejoint en cela l'auteur de l'avant-projet, que le droit d'accès implique que la personne concernée puisse prendre connaissance de la preuve de sa culpabilité ou de son innocence. Bien sûr, le droit d'accès tel qu'il est prévu dans l'avant-projet peut être assorti de conditions. Pour commencer, il est possible d'exiger de la personne concernée qu'elle indique dans sa requête dans le cadre de quel droit (fondamental) elle demande à pouvoir exercer son droit d'accès. En effet, l'avant-projet fait (à juste titre) une distinction entre d'une part le droit d'accès en vertu de l'article 38 §1er de la LPD, et d'autre part le droit d'accès dans le cadre des 'droits Franchimont'. Il est aussi possible d'exiger de la personne concernée qu'elle précise dans le cadre de quel lien elle formule cette requête. Le MP s'acquitte en effet de toute une série de missions qui ne présentent pas toutes un lien avec un dossier pénal (en cours). Cependant, prévoir que la personne concernée doive, dans le cadre du droit d'accès en vertu du Titre 2 de la LPD, pouvoir identifier concrètement et même *« précisément »* les pièces *« et les données à caractère personnel qu'elle contient »*[19] semble être une condition dont on peut douter qu'elle satisferait aux critères de la Cour de Justice de l'Union européenne. En outre, il convient de faire remarquer que la personne concernée n'a pas toujours connaissance du fait que le MP traite ses données à caractère personnel – loin de là –, ni a fortiori des données dont il s'agit.

20. On peut donc se demander si le législateur national peut déroger aux principes généraux définis à l'échelon européen pour les droits de contrôle de la personne concernée lorsque ceux-ci sont intégrés dans le cadre plus large des droits de la procédure pénale.

21. Comme nous le disions, l'avant-projet prévoit deux formes de droit d'accès (et d'autres droits fondamentaux): l'une reposant sur l'article 38 §1er de la LPD, et l'autre relevant des 'droits Franchimont'. Cependant, cela ne veut pas encore dire que l'article 44 de la LPD puisse être interprété comme donnant le droit d'associer le droit d'accès en vertu de la *LED* et du Titre 2 de la LPD, par analogie aux 'droits Franchimont', à une obligation de motivation ou de le soumettre à la condition que la personne concernée doive présenter des éléments permettant de conclure que ses données à caractère personnel sont traitées dans le cadre d'un dossier pénal[20]. Le COC est par conséquent d'avis que ce point de départ adopté par l'avant-projet est particulièrement douteux.

---

[17] Article 21bis §2, 2e alinéa du Code d'instruction criminelle.
[18] Article 21bis §5, premier alinéa du Code d'instruction criminelle. Voir le projet d'article 21bis/1 qui déclare les §§ 2 à 8 de l'article 21bis applicables (article 70 de l'avant-projet).
[19] Projet d'article 21bis/3 §1er, 3e alinéa du Code d'instruction criminelle.
[20] Strictement parlant, la personne concernée est uniquement tenue d'apporter la preuve de son identité. On peut donc se demander si le MP peut légitimement exiger que la personne concernée soit en mesure de démontrer (également) son intérêt à exercer ses droits fondamentaux. Le seul lien qui est en réalité exigé par le droit à la protection des données est le fait que le responsable du traitement traite réellement les données à caractère personnel de la personne concernée. Dans l'hypothèse

22. Le COC prie donc l'auteur de l'avant-projet de tenir compte lors de la transposition des droits de contrôle de la *LED*, transposés aux articles 36 à 39 inclus de la LPD, des remarques fondamentales ci-dessus qui démontrent qu'il n'existe pas du point de vue juridique de contradiction fondamentale entre d'une part les objectifs du droit à la protection des données et d'autre part l'objectif du droit de la procédure pénale. Globalement, il s'agit bel et bien de deux droits fondamentaux (équivalents) qui peuvent être mis en œuvre de manière complémentaire ou en parallèle, en fonction des objectifs respectifs. Il n'est toutefois pas exclu que ces deux droits fondamentaux, et donc les droits garantis découlant de l'article 8 de la Charte, d'une part, et ceux découlant des articles 47 et 48 de la Charte, d'autre part, puissent entrer en conflit et qu'il faille donc trouver un équilibre entre les deux. Cependant, ce conflit de droits fondamentaux ne doit pas pour autant être considéré comme une *« contradiction fondamentale »*.

2. Remarque générale concernant l'option de l'exercice direct des droits de contrôle à l'égard des traitements effectués par le ministère public et par les cours et tribunaux de droit commun

23. En ce qui concerne l'exercice des droits à l'information, d'accès, de rectification, d'effacement/de suppression et de limitation à l'égard des traitements de données, l'Organe de contrôle constate que l'auteur de l'avant-projet et donc le ministre de la Justice optent pour un système d'exercice **direct** de ces droits auprès du responsable du traitement. Ce choix, pourtant pertinent, contraste néanmoins fortement avec l'exercice des droits à l'égard des traitements effectués par les services de police (qui dans le cadre de l'information en matière pénale sont dans une très large mesure identiques à ceux du MP/du juge d'instruction), une matière dans laquelle le législateur – cédant à la pression des services de police – a opté (et opte toujours) pour un système d'accès **indirect** auprès de l'autorité de contrôle, à savoir le COC. Ce système d'accès indirect est depuis quelques années fortement sous pression et fait l'objet d'une procédure préjudicielle auprès de la Cour de Justice de l'Union européenne dans le sillage de deux questions préjudicielles posées par la Cour d'appel de Bruxelles dans son arrêt du 9 mai 2022 rendu dans l'affaire 'DD' et '*Ligue des Droits Humains'* contre le COC :

1. *« Les articles 47 et 8, §3 de la Charte des droits fondamentaux de l'Union européenne imposent-ils de prévoir un recours juridictionnel à l'encontre de l'autorité de contrôle indépendante telle que l'Organe de contrôle de l'information policière lorsqu'elle exerce les droits de la personne concernée à l'égard du responsable du traitement ? »*
2. *« L'article 17 de la Directive 2016/680 est-il conforme aux articles 47 et 8, §3 de la Charte des droits fondamentaux de l'Union européenne tels qu'ils sont interprétés par la Cour de justice en ce sens qu'il n'oblige l'autorité de contrôle – qui exerce les droits de la personne concernée envers le responsable du traitement – qu'à informer cette personne « qu'elle a procédé à toutes les vérifications nécessaires ou à un examen » et « de son droit de former un recours*

où la consultation d'un dossier fait passer à l'avant-plan les restrictions de l'article 15 de la *LED* (article 38 §2 de la LPD), il en est tenu compte dans l'avant-projet, mais le COC renvoie à ce sujet à l'avis de l'APD.

juridictionnel », alors que pareille information ne permet aucun contrôle a posteriori sur l'action et l'appréciation de l'autorité de contrôle au regard des données de la personne concernée et des obligations qui pèsent sur le responsable du traitement ? ».

Cette procédure soumet donc quoi qu'il en soit le système belge de l'accès indirect aux traitements de données effectués par la police, lequel constitue un cas unique au sein de l'Union européenne, à l'avis de la Cour de Justice de l'Union européenne quant à sa conformité à la Charte des droits fondamentaux de l'Union européenne et à la législation secondaire de l'Union européenne. Le verdict est attendu à l'automne de 2023. L'avis rendu par l'Avocat général Laila Medina[21] le 15 juin 2023 est d'ores et déjà particulièrement critique et même carrément négatif au sujet de ce système belge d'accès indirect, qui est pourtant défendu assidûment par l'État belge dans le cadre de cette procédure. L'Avocat général estime que le principe de base doit être l'accès direct auprès du responsable du traitement (fonctionnel). Le COC constate que l'auteur de l'avant-projet suit à juste titre ce principe de base.

Dans cette perspective plus large, il convient de se demander quel argument acceptable la police (et ses ministres de tutelle ?) peut encore alléguer en faveur du maintien de l'accès indirect aux traitements de données opérationnels effectués par la police à présent qu'il est établi qu'un droit à un exercice direct des droits susmentionnés est prévu notamment pour le MP et pour le juge d'instruction pour des traitements par essence identiques ou du moins analogues, si ce n'est – à juste titre – moyennant une application au cas par cas de restrictions de ce droit.

3. Commentaire par article

3.1. Article 21 de l'avant-projet : le Registre central des dossiers pénaux

24. L'avant-projet insère un nouvel article 564 dans le Code d'instruction criminelle et institue un Registre central des dossiers pénaux dans lequel tous les dossiers pénaux seront enregistrés et conservés. Outre les magistrats, les *« membres des services de police »* auront notamment accès au Registre central[22], pour autant qu'ils en aient besoin en vue de deux finalités :

a) pour assurer le suivi et/ou le contrôle de mesures adoptées par une autorité judiciaire (par ex. une arrestation, une fouille, un prélèvement d'ADN) et de mesures prises dans le cadre de la surveillance des personnes condamnées ou internées (par ex. le contrôle des mesures de probation);
b) pour assurer le suivi des actes d'enquête demandés à la requête (via une apostille) du magistrat dans un dossier pénal.

[21] Cour de Justice de l'Union européenne, C-333/22, https://www.curia.europa.eu.
[22] Projet d'article 564 §5, 2° du Code d'instruction criminelle.

Cet accès permet aux services de police d'une part de prendre connaissance de manière digitale des apostilles et d'autre part de rendre compte de manière digitale, par le biais du Registre central, des devoirs d'enquête ou missions de contrôle accompli(e)s[23].

25. En ce qui concerne les mesures adoptées pour des personnes condamnées ou internées, les services de police utilisent jusqu'ici *I+Belgium*[24] et l'application PSC[25] dans FOCUS[26] pour le suivi policier des mesures sur le terrain. I+Belgium génère un message automatique à l'intention du service DJO/VSS[27] de la police fédérale, qui est chargé de la saisie des signalements judiciaires dans la Banque de données nationale générale (BNG)[28]. Il en découle que la BNG contient actuellement à la fois des 'mesures policières' (des mesures imposées en toute autonomie par les services de police) et des 'mesures judiciaires' (pas toujours actualisées) (c'est-à-dire des mesures ordonnées par une autorité judiciaire), qui se limitent d'ailleurs actuellement à des mesures à l'égard de personnes condamnées ou internées et à des mesures à l'égard de la jeunesse.

26. L'Organe de contrôle est résolument partisan d'une centralisation de **toutes** les informations judiciaires dans une seule source unique (ou authentique). La création d'un Registre central des dossiers pénaux permettra de maintenir une distinction claire entre les 'mesures policières' saisies dans la BNG et les 'mesures judiciaires' saisies dans le Registre central des dossiers pénaux par les autorités judiciaires compétentes. Néanmoins, il peut également être utile de saisir la mesure judiciaire dans la BNG, encore qu'il serait préférable (à terme) de ne pas le faire trop souvent étant donné qu'il s'agit d'une double saisie. On peut par exemple penser à des cas urgents nécessitant une intervention très rapide des services de police, comme la saisie d'un véhicule volé. De même, il n'est pas toujours évident de faire une distinction stricte entre les mesures judiciaires et les mesures administratives, ces dernières devant être saisies dans la BNG.

27. Il sera par ailleurs important, pour une mise en œuvre efficace des mesures, d'aviser la police lorsqu'une nouvelle mesure ou une modification du statut est saisie dans le Registre central. L'Organe de contrôle suppose que la nouvelle application *JustSignal*, qui devrait d'ici peu remplacer *I+Belgium* (il est question du deuxième trimestre de 2024), constituera un premier élément dans la réalisation du Registre central des dossiers pénaux.

28. La numérisation des apostilles – soit dit en passant, par souci d'exhaustivité, il serait préférable d'un point de vue juridique d'utiliser le terme *« réquisition »* plutôt que le terme *« apostille »* dans le

---

[23] Exposé des motifs, p. 72.
[24] Le SPF Justice remplacera bientôt *I+Belgium* par *JustSignal*, une source authentique pour les signalements judiciaires.
[25] Afin de pouvoir utiliser sur le terrain les informations provenant de *I+Belgium*, une application spéciale a été développée dans FOCUS : l'application 'Personnes sous Conditions' (PSC).
[26] FOCUS est une application mobile qui permet à un fonctionnaire de police sur le terrain d'accéder rapidement aux banques de données et applications policières sécurisées.
[27] Direction centrale des opérations de police judiciaire, Service des saisies et signalements.
[28] COL 03/2020 Directives provisoires relatives à l'utilisation de la plate-forme informatique *« I+Belgium »*, Circulaires | Ministère public (om-mp.be), p. 4.

sillage de la terminologie qui existe dans la LFP[29] – aura en outre pour effet de faciliter et d'accélérer fortement la collaboration avec la police. Cette numérisation pourra également être combinée à l'obligation, pour les services de police, de saisir un 'motif de consultation'. On peut par exemple penser à la situation dans laquelle l'accès aux images des caméras peut être autorisé un mois après leur enregistrement uniquement si la référence d'une réquisition numérique valable via une apostille est complétée en tant que motif de consultation conformément à l'article 25/7 §1er, 2e alinéa de la LFP.

3.2. Article 35 de l'avant-projet : le système de gestion des dossiers

29. L'avant-projet insère dans le Code judiciaire un article 725*ter* qui institue auprès du Service Public Fédéral Justice un système de gestion des dossiers numériques.

« §2. Ce système de gestion des dossiers a pour finalités :

*1° **permettre l'accès au dossier numérique**, conformément aux Codes judiciaire et d'instruction criminelle et aux lois particulières relatives à la procédure civile et pénale ainsi qu'à leurs arrêtés d'exécution :*

a) pour les personnes qui exercent une fonction judiciaire visée à la deuxième partie, livre II, titre 1er, et les magistrats en formation visés à l'article 259octies, §1er, alinéa 4 ;

***c) sur la base de l'article 646 du Code d'instruction criminelle, à la Banque de données Nationale Générale** visée à l'article 44/7 de la loi sur la fonction de police, uniquement pour les données visées au §3, 4°[30] ;*

***d) sur la base de l'article 28, 4° de la loi du 30 juillet 2018** relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, **aux banques de données de base**, visées à l'article 44/11/2, §6 de la loi sur la fonction de police, uniquement pour les données visées au §3, 4° ; (…) »*

30. Ce système de gestion des dossiers offre une solution pour le flux (de préférence automatisé) de la justice vers la police qui est prévu à l'article 646 du Code d'instruction criminelle, lequel est entré en vigueur le 7 avril 2018 mais n'a jusqu'ici toujours pas été mis en œuvre (sur le plan technique). Ce flux permettrait aux services de police d'adapter et d'actualiser la BNG en fonction de la suite judiciaire donnée telle que prévue à l'article 44/5 §6 de la LFP[31]. Selon l'exposé des motifs, les métadonnées gardées concernant le statut des dossiers et des personnes qui s'y trouvent serviront notamment à mettre à jour la BNG et les banques de données de base. Le service de police en charge de l'enquête

[29] Voir la section 4 du chapitre II. Le terme « apostille » fait référence au support matériel de la réquisition et n'est pas un terme légal usuel.
[30] Les données visées au §3, 4° sont *« le statut du dossier et celui des personnes y enregistrées »*.
[31] *« §6. Lorsque la police a connaissance, par elle-même, par la personne concernée ou son avocat, en application de l'article 646 du Code d'instruction criminelle ou par tout autre moyen, du fait que les données ne sont plus exactes ou ne remplissent plus les conditions pour être traitées dans le cadre des §§ 1er, 3 ou 4, ces données sont mises à jour. »*

devrait également recevoir ces métadonnées automatiquement par le biais de cette application[32]. L'auteur de l'avant-projet se limite ici aux métadonnées 'statut des dossiers' et 'personnes qui s'y trouvent'. L'exposé des motifs ne permet pas d'établir pourquoi l'auteur de l'avant-projet se limite à ces métadonnées, mais cela semble suffire pour les adaptations visées.

Le COC n'a pas d'autres remarques spécifiques à formuler au sujet de l'objectif et de la teneur de cet article[33]. Il espère au contraire que ces mesures envisagées vont enfin pouvoir être mises en œuvre de manière à ce que les services de police puissent eux aussi – bien plus qu'actuellement – satisfaire à leurs obligations en matière de protection des données, dont le principe d'exactitude[34]. En effet, répétons-le, la BNG à elle seule contient encore un nombre (trop) important d'enregistrements inexacts – comme le COC l'a encore démontré à plusieurs reprises dans ses derniers rapports d'activité[35] – qui ont souvent un impact direct sur le citoyen en termes de traitement par la police, d'accès à certaines fonctions ou offices, d'obtention ou non d'une attestation, d'un avis ou d'une habilitation de sécurité, etc.

3.3. Article 83 de l'avant-projet : références dactyloscopiques dans le Casier judiciaire central

31. L'article 590 du Code d'instruction criminelle énumère les données à caractère personnel qui sont enregistrées dans le Casier judiciaire central. L'article 83 de l'avant-projet souhaite y insérer les deux alinéas suivants :

« Outre les données à caractère personnel visées à l'alinéa 1er, les références dactyloscopiques uniques visées dans l'arrêté royal du 11 mars 2019 relatif aux modalités d'interrogation directe de la Banque de données nationale générale visée à l'article 44/7 de la loi sur la fonction de police au profit du Service public fédéral Justice dans le but de contribuer à l'identification unique des détenus, si elles sont disponibles, sont enregistrées et traitées par le Casier judiciaire au profit des autorités et des personnes visées à l'article 589, alinéa 2, 4°, et à l'article 593 du présent code.[36]

Concernant les ressortissants d'un pays tiers au sens de l'article 3 du Règlement (UE) 2019/816 du Parlement européen et du Conseil portant création d'un système centralisé permettant d'identifier les États membres détenant des informations relatives aux condamnations concernant des ressortissants de pays tiers et des apatrides (Ecris-TCN), qui vise à compléter le système européen d'information sur les casiers judiciaires, et modifiant le Règlement (UE) 2018/1726, les données biométriques visées à l'article 44/1, §2, 1°, de la loi sur la fonction de police sont demandées par le Casier judiciaire au service de police compétent au moyen d'une référence dactyloscopique unique et supprimées sans

[32] Exposé des motifs, p. 89-90.
[33] Si ce n'est la nécessité d'une adaptation linguistique de la construction de phrase du projet d'article 725*ter* §2, 1°, c) et d), qui ne semble pas tout à fait correcte.
[34] Cf. article 28, 4° de la LPD.
[35] Voir les rapports d'activité de 2022, 2021, 2020 et 2013-2019 sur le site www.organedecontrole.be.
[36] Soulignement du COC.

délai du Casier judiciaire après que ces données ont été transmises conformément à l'article 5 du Règlement. ».

32. L'avant-projet prévoit donc aussi la possibilité de traiter des empreintes digitales dans le Casier judiciaire central. Cette modification est proposée en application du système européen d'information ECRIS-TCN[37], de manière à permettre l'échange d'informations, dont des empreintes digitales, de ressortissants d'un pays tiers figurant dans les casiers judiciaires des différents États membres.

33. L'article 44/11/7 de la LFP permet la transmission de données policières aux autorités judiciaires compétentes pour leur permettre d'exercer leurs missions légales. Les empreintes digitales sont demandées au service BIS[38] de la police judiciaire fédérale, pour autant qu'elles soient disponibles conformément à l'article 44/11/12 §2 de la LFP et à l'arrêté royal du 11 mars 2019[39]. Le COC n'a pas de remarques spécifiques à formuler concernant ce traitement.

34. Le deuxième alinéa précise que les empreintes digitales reçues ne peuvent être conservées que pour la durée nécessaire à l'envoi des données à l'ECRIS-TCN et doivent ensuite être supprimées sans délai[40].

L'avant-projet n'indique cependant pas clairement si les empreintes digitales peuvent uniquement être traitées en vue de l'échange dans le cadre de la Convention européenne, ou aussi en vue d'autres finalités. Le premier alinéa stipule en effet : *« Outre les données à caractère personnel visées à l'alinéa 1er, les références dactyloscopiques uniques (…) sont enregistrées et traitées par le Casier judiciaire au profit des autorités et des personnes visées à l'article 589, alinéa 2, 4°, et à l'article 593 du présent code.[41] ».*

Cela pourrait signifier que les autorités et personnes qui ont accès au Casier judiciaire en vertu de la loi pourraient aussi traiter les références dactyloscopiques en vue de leurs propres finalités. Il appartient à l'auteur de l'avant-projet de définir dans l'avant-projet la (les) finalité(s) du traitement des références dactyloscopiques dans le Casier judiciaire central.

PAR CES MOTIFS,

[37] Article 5 du Règlement européen 2019/816 du 17 avril 2019 portant création d'un système centralisé permettant d'identifier les États membres détenant des informations relatives aux condamnations concernant des ressortissants de pays tiers et des apatrides (ECRIS-TCN), qui vise à compléter le système européen d'information sur les casiers judiciaires, et modifiant le règlement (UE) 2018/1726, *JOUE* 22 mai 2019, L135/1.
[38] Le Biometric Identification Service (BIS) est un service de la Direction centrale de la police technique et scientifique (DJT).
[39] A.R. du 11 mars 2019 relatif aux modalités d'interrogation directe de la Banque de Données nationale générale visée à l'article 44/7 de la loi sur la fonction de police.
[40] Exposé des motifs, p. 245.
[41] Les personnes qui ont accès au Casier judiciaire en vertu de la loi sont les magistrats du ministère public, les juges d'instruction, la magistrature assise, certains fonctionnaires, les membres des services de police, etc.

l'Organe de contrôle de l'information policière

prie le demandeur de tenir compte des remarques susmentionnées.

Avis approuvé par l'Organe de contrôle de l'information policière le 5 septembre 2023.

Pour l'Organe de contrôle,
Le Président *a.i.*,
Frank SCHUERMANS (SIGNÉ)