COMMISSION NATIONALE
DE L'INFORMATIQUE ET DES LIBERTÉS

PLAINTE AU TITRE DE L'ARTICLE 38 DE LA LOI N° 78-17 DU 6 JANVIER 1978

POUR :

1°) **L'association « La Quadrature du Net » (LQDN), association régie par la loi du 1er juillet 1901 dont le siège social est situé au 115, rue de Ménilmontant à Paris (75020), enregistrée en préfecture de police de Paris sous le numéro W751218406, représentée par [redacted], membre du collège solidaire en exercice**

2°) **Les 15 248 plaignants ayant mandaté La Quadrature du Net**

CONTRE : **Le ministre de l'intérieur**

Table des matières

Procédure **3**

Discussion **5**

I Sur l'illégalité des données collectées par le ministère de l'intérieur **5**

A. En ce qui concerne le cadre juridique 5

1. S'agissant du code de procédure pénale 5

2. S'agissant du droit des données personnelles 7

B. En ce qui concerne les pratiques illégales constatées 10

1. S'agissant de l'absence d'exactitude et de pertinence des données collectées 11

2. S'agissant de la collecte en dehors des critères fixés par la loi 14

II Sur l'illégalité de l'accès au TAJ **16**

A. En ce qui concerne le cadre juridique 16

B. En ce qui concerne les illégalités constatées 18

III Sur l'accès au TAJ par reconnaissance faciale **20**

A. En ce qui concerne le cadre juridique 20

1. S'agissant du code de procédure pénale 20

2. S'agissant du droit des données personnelles 21

a. Nécessité d'une base légale 22

b. Atteinte à l'essence du droit 25

c. Exigence de proportionnalité 27

B. En ce qui concerne les faits reprochés 31

1. S'agissant de l'absence de base légale 33

2. S'agissant de l'atteinte à l'essence du droit à la vie privée 35

3. S'agissant de l'absence de nécessité absolue 37

Bordereau des productions **44**

PROCÉDURE

1. Aux termes de l'article 38 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (ci-après « loi Informatique et Libertés ») :

> « *Toute personne peut mandater* […] *une association ou une organisation dont l'objet statutaire est en relation avec la protection des droits et libertés lorsque ceux-ci sont méconnus dans le cadre d'un traitement de données à caractère personnel* […] *aux fins d'exercer en son nom les droits prévus aux articles 77 à 79 et 82 du règlement (UE) 2016/679 du 27 avril 2016. Elle peut également les mandater pour agir devant la Commission nationale de l'informatique et des libertés, contre celle-ci devant un juge ou contre le responsable de traitement ou son sous-traitant devant une juridiction lorsqu'est en cause un traitement relevant du titre III de la présente loi.* »

2. De même, aux termes du 1 de l'article 77 du règlement UE n° 2016/679 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 (ci-après « RGPD ») :

> « *Sans préjudice de tout autre recours administratif ou juridictionnel, toute personne concernée a le droit d'introduire une réclamation auprès d'une autorité de contrôle, en particulier dans l'État membre dans lequel se trouve sa résidence habituelle, son lieu de travail ou le lieu où la violation aurait été commise, si elle considère que le traitement de données à caractère personnel la concernant constitue une violation du présent règlement.* »

3. La Quadrature du Net est une association de loi 1901 déclarée en préfecture le 5 février 2013. Elle prévoit dans ses statuts que « *l'Association a pour objet désintéressé et non lucratif la promotion et la défense des droits et des libertés fondamentales dans l'environnement numérique* », notamment, « *la promotion et la défense du droit à l'intimité, à la vie privée, à la protection de la confidentialité des*

communications et du secret des correspondances et à la protection des données à caractère personnel » et « *la lutte contre la surveillance généralisée ou politique, d'origine privée ou publique* ».

4. Du 24 mai au 24 septembre 2022, en application de l'article article 38 de la loi Informatique et Libertés, La Quadrature du Net a invité tout individu résidant en France à la mandater via son site `https://technopolice.fr/plainte` pour qu'il exerce, en son nom, les droits que lui confère l'article 38 de la loi Informatique et Libertés afin d'introduire la présente réclamation devant la Commission nationale de l'informatique et des libertés (ci-après « la CNIL »).

5. 15 248 plaignants ont ainsi mandaté La Quadrature du Net pour ce faire (la liste de leurs noms est jointe en annexe, *cf.* pièce n° 1).

DISCUSSION

6. Conformément à l'article R. 40-23 du code de procédure pénale, le ministre de l'intérieur est responsable du traitement automatisé de données personnelles dénommé « Traitement des antécédents judiciaires » (ci-après « TAJ »). Les finalités de ce traitement sont définies à l'article 230-6 du même code.

7. Les services de police et de gendarmerie peuvent mettre en œuvre le TAJ dans les conditions fixées à ces articles ainsi qu'aux dispositions des sections du code de procédure pénale dans lesquelles elles sont insérées. Ce cadre prévoit notamment les conditions de collecte de données et d'accès au traitement, en particulier par d'autres acteurs tels que les services de renseignement.

8. Par la présente plainte, La Quadrature du Net et les 15 248 personnes concernées par ce traitement et l'ayant mandatée pour agir en leur nom entendent contester la pratique de fichage de masse qui est aujourd'hui effectuée à partir du TAJ, ainsi que l'utilisation illégale, dangereuse et totalement banalisée de la reconnaissance faciale promue par le ministre de l'intérieur, et faite à partir de ce traitement.

9. Il sera démontré que la mise en œuvre du TAJ par la police et la gendarmerie, ainsi que par les services de renseignement, est illégale, et ce sur trois aspects : la collecte des données traitées (I), l'accès au traitement de façon générale (II) et l'accès au traitement par des outils de reconnaissance faciale (III).

I. Sur l'illégalité des données collectées par le ministère de l'intérieur

A. En ce qui concerne le cadre juridique

1. S'agissant du code de procédure pénale

10. Les articles 230-6 et 230-7 du code de procédure pénale prévoient que le TAJ peut contenir des données personnelles recueillies :

— lors d'enquêtes préliminaires et de flagrance ou de commissions rogatoire concernant tout crime et délit, ainsi que les conventions de cinquième classe mentionnées à l'article R. 40-25 du code de procédure pénale ;

— concernant des personnes à l'encontre desquelles il existe des indices graves ou concordants rendant vraisemblable qu'elles aient pu participer, comme auteurs ou complices, à la commission de ces infractions ;

— concernant les victimes de ces infractions.

11. Les informations recueillies dans le TAJ doivent donc être uniquement liées à des procédures judiciaires et collectées dans le cadre de ces procédures. En outre, l'article 230-6 prévoit que ce traitement a pour finalités de faciliter la constations des infractions à la loi pénale, le rassemblement des preuves de ces infractions et la recherches de leurs auteurs.

12. L'article R. 40-26 du code de procédure pénale liste exhaustivement les données « *pouvant* » être enregistrées pour atteindre les finalités du TAJ.

13. En outre, l'article 230-8 du même code prévoit qu'une fois les données collectées, le procureur de la République territorialement compétent peut contrôler leur exactitude et leur mise à jour et peut ordonner d'office « *qu'elles soient effacées, complétées ou rectifiées, notamment en cas de requalification judiciaire, ou qu'elles fassent l'objet d'une mention* ». Il prévoit également que les données personnelles concernant les personnes mises en cause :

— sont effacées en cas de décision de relaxe ou d'acquittement devenue définitive sauf si le procureur de la République en prescrit le maintien, auquel cas elles font l'objet d'une mention ;

— font l'objet d'une mention en cas de décision de non-lieu ou de classement sans suite, sauf si le procureur de la République ordonne leur effacement.

14. À ce contrôle s'ajoute celui prévu par l'article R. 40-32 du code de procédure pénale qui dispose que « *La mise en œuvre et la mise à jour du traitement sont contrôlées par un magistrat du parquet hors hiérarchie, désigné pour trois ans par arrêté du garde des sceaux, ministre de la justice, et assisté par un comité composé de trois membres nommés dans les mêmes conditions.* »

15. L'ensemble de ces pouvoirs s'exercent sans préjudice du contrôle exercé par la CNIL en vertu des articles 19, 51 et 108 de la loi Informatique et Libertés. Celle-ci est en effet compétente pour contrôler la légalité de la mise en œuvre du traitement ainsi que le respect, par le ministre de l'intérieur, de ses obligations résultant du RGPD, de la loi Informatique et Libertés et de la directive UE n° 2016/680 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 (ci-après directive « police-justice »).

2. S'agissant du droit des données personnelles

16. Aux termes de l'article 4 de la loi Informatique et Libertés, les données personnelles doivent être :

> « *1° Traitées de manière licite, loyale et, pour les traitements relevant du titre II, transparente au regard de la personne concernée ;*
>
> *2° Collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités.* [...]
>
> *3° Adéquates, pertinentes et, au regard des finalités pour lesquelles elles sont traitées, limitées à ce qui est nécessaire ou, pour les traitements relevant des titres III et IV, non excessives ;*
>
> *4° Exactes et, si nécessaire, tenues à jour. Toutes les mesures raisonnables doivent être prises pour que les données à caractère personnel qui sont inexactes, eu égard aux finalités pour lesquelles elles sont traitées, soient effacées ou rectifiées sans tarder ;*
>
> [...] »

17. Ces principes généraux doivent être interprétés à la lumière de la jurisprudence du droit de l'Union européenne et de la Convention européenne des droits de

l'homme et des libertés fondamentales (ci-après « CESDH »).

18. En matière de surveillance, la Cour de justice de l'Union européenne (CJUE) a rappelé, en se fondant notamment sur la Charte des droits fondamentaux de l'Union européenne (ci-après la « Charte »), que « *pour satisfaire à l'exigence de proportionnalité, une réglementation 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 sont concernées disposent de garanties suffisantes permettant de protéger efficacement ces données contre les risques d'abus.* [...] *Ces considérations valent en particulier lorsqu'est en jeu la protection de cette catégorie particulière de données à caractère personnel que sont les données sensibles* » (*cf.* CJUE, gr. ch., 6 octobre 2020, *La Quadrature du Net e. a.*, aff. C-511/18 et C-512/18, pt. 132).

19. Au stade de la collecte des données, elle précise ainsi que celle-ci doit « *toujours répondre à des critères objectifs, établissant un rapport entre les données à conserver et l'objectif poursuivi. En particulier, de telles conditions doivent s'avérer, en pratique, de nature à délimiter effectivement l'ampleur de la mesure et, par suite, le public concerné* » (*cf.* CJUE, gr. ch., 21 décembre 2016, *Tele2 Sverige AB et Tom Watson e. a.*, aff. C-203/15 et C-698/15, pt. 110).

20. La Cour ajoute que « *s'agissant de la délimitation d'une telle mesure quant au public et aux situations potentiellement concernés, la réglementation nationale doit être fondée sur des éléments objectifs permettant de viser un public dont les données sont susceptibles de révéler un lien, au moins indirect, avec des actes de criminalité grave, de contribuer d'une manière ou d'une autre à la lutte contre la criminalité grave ou de prévenir un risque grave pour la sécurité publique*.» (même arrêt, pt. 111)

21. De même, pour la Cour européenne des droits de l'homme (CEDH), « *la protection des données à caractère personnel joue un rôle fondamental pour l'exercice du droit au respect de la vie privée et familiale consacré par l'article 8 de la Convention. La législation interne doit donc ménager des garanties appropriées pour empêcher toute utilisation de données à caractère personnel qui ne serait pas conforme aux garanties prévues dans cet article. Cette nécessité se fait d'autant plus sentir lorsqu'il s'agit de protéger les données à caractère personnel soumises à un traitement automatique, en particulier lorsque ces données sont utilisées à*

des fins policières. Le droit interne doit notamment s'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 de nature à protéger efficacement les données à caractère personnel enregistrées contre les usages impropres et abusifs » (*cf.* CEDH, 18 septembre 2014, *Brunet c. France*, n° 21010/10, § 35).

22. En application de ce principe, elle ainsi pu juger que même si le système de Traitement des infractions constatées (STIC), le fichier antérieur à 2012 de la police nationale relatif aux antécédents judiciaires, ne comportait « *ni les empreintes digitales* [...] *ni le profil ADN des personnes,* [ces données] *présentent néanmoins un caractère intrusif non négligeable, en ce qu'elles font apparaître des éléments détaillés d'identité et de personnalité en lien avec des infractions constatées, dans un fichier destiné à la recherche des infractions.* » (même arrêt, § 39)

23. Ainsi, la collecte de données doit toujours être en lien avec l'objectif poursuivi, selon des critères stricts de pertinence et de nécessité, permettant de réduire l'atteinte aux droits.

24. En outre, en ce qui concerne la suppression des données, la CEDH insiste sur le fait que, lorsque la base légale du traitement poursuit une finalité policière, cette suppression ne doit pas être d'une complexité excessive : « *Il serait totalement contraire à la nécessité de protéger le droit à la vie privée consacré par l'article 8 qu'un État puisse créer une base de données dans laquelle il serait difficile d'examiner ou de modifier les données, puis qu'il puisse invoquer la manière dont cette base de données a été conçue pour justifier son refus de supprimer des informations y figurant* » (*cf.* CEDH, *Catt c. Royaume-Uni*, 24 janvier 2019, n° 43514/15, pt. 127 [1]).

25. De la même manière, l'absence de garanties effectives pour obtenir l'effacement des données personnelles lorsqu'elles n'apparaissent plus pertinentes au regard de la finalité du fichier est particulièrement préoccupante s'agissant des caté-

1. Traduction non officielle faite par le greffe de la Cour dans le *Guide sur la jurisprudence de la Convention européenne des droits de l'homme relative aux données personnelles*, 2022, pt. 214, URL : `https://www.echr.coe.int/Documents/Guide_Data_protection_FRA.pdf`

gories sensibles des données personnelles conservées, qui appellent une protection accrue (même arrêt, § 123). Sur ce point, la Cour est « *particulièrement attentive au risque de stigmatisation de personnes qui* [...] *n'ont été reconnues coupables d'aucune infraction et sont en droit de bénéficier de la présomption d'innocence. Si, de ce point de vue, la conservation de données privées n'équivaut pas à l'expression de soupçons, encore faut-il que les conditions de cette conservation ne leur donne pas l'impression de ne pas être considérés comme innocents* » (*cf.* CEDH, 18 septembre 2014, *Brunet c. France*, préc., § 37).

26. La conservation de données non pertinentes peut en effet avoir une incidence sur les droits des personnes concernées par le traitement. Ainsi, dans l'affaire *M.M. c. Royaume-Uni* relative à la conservation à vie d'un avertissement sur le casier judiciaire d'un individu et à la divulgation de ces données à un futur employeur dans le cadre d'une recherche d'emploi, la Cour a mis en cause les défaillances dans la procédure destinée à réglementer l'accès des tiers aux antécédents judiciaires des personnes briguant un emploi, qui ne permettait aucune appréciation, à quelque stade que ce soit, de la pertinence des données pour l'emploi brigué ou pour savoir si le sujet des données pouvait être perçu comme continuant à présenter un risque (*cf.* CEDH, 13 novembre 2012, *M.M. c. Royaume-Uni*, n° 24029/07, § 204) [2].

27. Ainsi, ces exigences de proportionnalité et de minimisation des données s'appliquent aussi bien au moment de la collecte des données que tout au long de leur maintien au sein du fichier TAJ. Les policiers et les gendarmes sont donc tenus d'apprécier pour chaque donnée si, en fonction de leur nature et de leur contexte, elles peuvent avoir un lien direct avec la finalité du traitement. Ils ont également l'obligation de les supprimer dès lors que cela apparaît nécessaire, afin de réduire l'atteinte aux droits des personnes concernées.

B. En ce qui concerne les pratiques illégales constatées

28. En pratique, le ministre de l'intérieur met en œuvre le TAJ en violation des principes exposés ci-dessus car, d'une part, le traitement contient des données non pertinentes, inexactes et qui ne sont pas mises à jour (1) et, d'autre part, il est avéré

2. Voir plus précisément le point 226 du *Guide sur la jurisprudence de la Convention européenne des droits de l'homme relative aux données personnelles*.

que les agents de police et de gendarmerie procèdent à une collecte de données dans des situations qui ne sont pas prévues par la loi (2).

1. S'agissant de l'absence d'exactitude et de pertinence des données collectées

29. **En premier lieu**, la mise en œuvre du TAJ est illégale en ce que le fichier comporte de nombreuses fiches et données personnelles incorrectes ou qui auraient dues être supprimées au regard du contexte de leur collecte et du délai de conservation qui leur est associées.

30. En effet, dans un rapport d'information de deux députés de 2018 sur les fichiers mis à la disposition des forces de sécurité [3], ses auteurs constatent à de nombreuses reprises le caractère inexact des données conservées :

> « *Un certain nombre d'inexactitudes subsistent notamment dans le TAJ. Celui-ci est parfois rempli dans la précipitation par les fonctionnaires de police ou les militaires de la gendarmerie. Il arrive ainsi que des victimes soient enregistrées par erreur en qualité d'auteurs. La saisie incomplète ou imprécise des informations ou le défaut d'enrichissement des données peuvent être source d'alimentation de données de mauvaise qualité. À titre d'exemple, lorsqu'un fonctionnaire omet de remplir le champ "*mode opératoire*", l'alimentation du TAJ est imparfaite et cela limite ensuite les capacités de recoupements offertes par ce fichier. De même, il peut arriver que, pour décrire la nature de l'infraction concernée, il soit fait usage d'un terme usuel, tel que "*cambriolage*", qui ne correspond pas à une qualification juridique précise. Ce type d'erreurs est susceptible d'entraîner en particulier dans le TAJ, le FAED ou le FNAEG un dépassement des délais réglementaires de conservation des données.* »

31. Les auteurs de ce rapport attestent également du retard pris pour la mise à

3. Didier Paris, Pierre Morel-À-L'Huissier, *Rapport d'information sur les fichiers mis à la disposition des forces de sécurité*, 17 octobre 2018, URL : https://www.assemblee-nationale.fr/dyn/15/rapports/cion_lois/l15b1335_rapport-information.pdf

jour des suites judiciaires favorables et mentionnent les propos du procureur de la République près le tribunal de grande instance de Vienne qui précise que « *en l'état de leurs moyens humains, il est également parfaitement illusoire d'exiger du greffe la vérification effective des mises à jour opérées dans le TAJ* ». Ils concluent que « *faute de moyens adéquats, la transmission des suites judiciaires, le traitement des requêtes en effacement et la vérification des modifications effectuées ne constituent manifestement pas une priorité pour les parquets.* »

32. Cette absence, en pratique, de contrôle de l'exactitude des données conservées dans le TAJ, alors que cette prérogative est prévue par la loi est difficile à contester dans les faits. D'une part, elle s'explique selon les députés par un manque de compétence :

> « *On remarque par ailleurs que les procureurs tendent, peut-être du fait d'une maîtrise insuffisamment précise des dispositions de l'article 230-8, à demander systématiquement l'effacement et à faire peu usage de la faculté qui leur est offerte d'ordonner simplement l'inscription d'une mention au TAJ.* »

33. D'autre part, ce sont les procureurs de la République eux-mêmes qui, délibérément, refusent de mettre à jour le TAJ. Ainsi, Paul Michel, ancien procureur général de Grenoble explique sans filtre [4] :

> « *J'ai rarement fait droit à ces requêtes. On n'a pas intérêt à effacer rapidement les données issues des procédures. Le TAJ est un fichier qui permet de faire des rapprochements entre les procédures, de connaître l'ensemble des activités d'une personne de nature à permettre l'élucidation d'un certain nombre d'affaires. Il ne faut pas avoir avoir une vision simpliste, les fichiers sont utiles pour élucider des affaires très anciennes.* »

34. Plutôt que d'aider spécifiquement et de façon circonscrite à la résolution d'enquête, le fichier TAJ contient tellement de données sur les antécédents qu'il est

4. Interview au journal L'Essor Loire, 3 septembre 2018, URL : `https://www.lessor42.fr/paul-michel-la-tache-des-parquets-est-devenue-tres-lourde-21592.html`

utilisé pour retracer le parcours judiciaire d'une personne. Ainsi, les données ne sont pas recueillies pour favoriser la constatation des infraction et la recherches de leurs auteurs mais pour être, de façon large, utiles aux enquêteurs dans leurs quotidien. Il n'y a ni minimisation, ni proportionnalité, ni limitation au strict nécessaire, au détriment du droit des personnes concernées.

35. Les députés admettent clairement le dévoiement de la finalité première du TAJ :

> « *Malgré cette garantie [d'effacement prévues par les textes],* ***la consultation du TAJ dans le cadre d'enquêtes administratives soulève plusieurs difficultés****.*
>
> *Comme l'a souligné M. Rémy Heitz, directeur des affaires criminelles et des grâces,* ***le TAJ s'éloigne de sa finalité première*** *– faciliter la constatation des infractions à la loi pénale, le rassemblement des preuves de ces infractions et la recherche de leurs auteurs –* ***pour se rapprocher du rôle du casier judiciaire****.*
>
> *Si les rapporteurs prennent acte de cette évolution, liée à l'extension du champ des enquêtes administratives, ils estiment d'autant plus nécessaire de renforcer la fiabilité des informations contenues dans ce fichier. Le fait que le TAJ contienne* ***de nombreuses informations inexactes*** *(erreurs diverses, absence de prise en compte de suites judiciaires favorables par l'effacement des données ou l'ajout d'une mention) peut en effet avoir des* ***conséquences extrêmement lourdes pour les personnes concernées*** *par une enquête administrative.* »[5]

36. Les députés concluent en affirmant qu'«*il reste que des dizaines de milliers de fiches demeurent à mettre à jour en particulier dans le TAJ, le FAED et le FNAEG. Les insuffisances de cette mise à jour ne sont pas acceptables au regard des libertés publiques, eu égard notamment aux conséquences qu'elles peuvent avoir sur l'accès à certains emplois faisant l'objet d'enquêtes administratives.* »

37. En effet, dès lors que le TAJ est consulté dans le cadre d'enquêtes administratives, une mention au sein de ce fichier peut empêcher l'accès à un emploi ou au

5. En gras dans le texte.

droit à un titre de séjour.

38. **Il en résulte que** le ministre de l'intérieur, en tant que responsable de traitement conformément à l'article R. 40-23 du code de procédure pénale, porte une atteinte excessive et disproportionnée aux droits et libertés des personnes concernées au stade de la collecte et de la mise à jour des données traitées dans le TAJ. Cette atteinte renouvelée est injustifiable et remet en cause à elle seule l'existence de ce fichier qui ne semble pas pouvoir fonctionner en pratique sans violer à plusieurs reprises non seulement les dispositions du code de procédure pénale mais également les principes généraux des données personnelles.

2. S'agissant de la collecte en dehors des critères fixés par la loi

39. **En deuxième lieu**, la mise en œuvre du TAJ est illégale en ce qu'elle consiste à traiter des données sans base légale.

40. En effet, il a été constaté à plusieurs reprises que la police nationale et la gendarmerie recueillent des données pour les besoins du TAJ en dehors de toute enquête de flagrance, préliminaire ou de commission rogatoire, contrairement à ce qui est prévu par le cadre législatif et réglementaire.

41. Ainsi, il est documenté depuis plusieurs années que les agents de police et de gendarmerie prennent en photographie avec des téléphones personnels et non des équipements officiels, les cartes d'identité de personnes dont ils contrôlent l'identité dans le cadre de missions de police administrative.

42. Par exemple, le journal Le Monde [6] constatait dès 2019 que la vérification de pièces d'identité par des gendarmes s'accompagne « *à plusieurs reprises* [de] *gendarmes prenant en photo cartes d'identité et passeports avec leur smartphone.* » Le journal prouve également que, contrairement à ce que répondait la gendarmerie, ces opérations n'étaient pas opérées par le système Neogend dans le

6. Aline Leclerc, « "Gilets jaunes" : quand la gendarmerie prend en photo les cartes d'identité des manifestants », Le Monde, 2 mars 2019, URL : https://www.lemonde.fr/societe/article/2019/03/02/gilets-jaunes-quand-la-gendarmerie-prend-en-photo-les-cartes-d-identite-des-manifestants_5430569_3224.html

cadre d'une consultation autorisée de fichiers dès lors qu'il s'agissait de téléphones (iPhone d'Apple) sur lesquels le système Neogend ne fonctionne pas :

> « *« En aucun cas Neogend ne peut fonctionner sur ce modèle : les versions modifiées du système d'exploitation iOS n'existent pas. L'utilisation d'un iPhone pose un second problème car ce sont les marques Samsung et Sony qui ont remporté les appels d'offres pour équiper la gendarmerie : le gendarme utilise vraisemblablement son téléphone personnel. Cette même photo montre par ailleurs l'utilisation de l'application « photo » d'Iphone – il ne s'agit pas de scan. Et le gendarme n'a pas consulté de fichier dans la foulée.* »

Ces pratiques ne sont pas isolées, comme le démontre de façon très exhaustive, un billet de blog du journaliste Ricardo Parreira [7] :

> « *Depuis plusieurs mois, a fortiori au cours des manifestations, la presse nationale, a publié à plusieurs reprises des articles relatant* ***les agissements de certains policiers*** *dans l'exercice de leurs fonctions, plus précisément lors de* ***vérifications d'identité****, ou d'opérations à proximité de manifestants. Ces agents de la paix prenaient, à l'aide de* ***smartphones personnels****, des* ***photographies de cartes d'identité ou bancaires****, mais aussi des* ***visages de manifestants comme d'acteurs de la presse ou de vidéastes****.* » [8]

43. Plusieurs exemples à Montpellier le 23 février 2019, à Bordeaux les 28 et 30 mars 2019, à Toulouse le 12 mai 2019 ou encore à Montpellier le 25 mai 2019, démontrent une pratique installée de collecte par les policiers de données nominatives ou de photographies. Ces pratiques sembleraient avoir pour but d'alimenter des traitements de données utilisés par la police et la gendarmerie, en premier lieu duquel le TAJ, qui est – comme il sera démontré – utilisé très régulièrement par la police, notamment à des fins de contrôle d'identité.

7. Ricardo Parreira, « Police & Tech – Fichage dissimulé, libertés piétinées », Le Club de Mediapart, 23 décembre 2020, URL : `https://blogs.mediapart.fr/ricardo-parreira/blog/211220/police-tech-fichage-dissimule-libertes-pietinees`

8. En gras dans le texte.

44. Des exemples plus récents peuvent facilement être trouvés sur les réseaux sociaux. À titre d'exemple :

— un policier qui prend en vidéo une personne qui s'exprime dans la rue à Choisy-le-Roi le 20 septembre 2022 [9] ;
— un policier filmant le visage de manifestants à Paris le 10 septembre 2022 [10].

45. **Il en résulte que** des données sont traitées dans le TAJ sans avoir été prévues par le cadre réglementaire ou législatif.

46. Au regard de ses prérogatives de contrôle, la CNIL pourra procéder à un examen des fiches et des données contenues dans le TAJ pour vérifier la légalité des données qui y sont collectées et notamment si celles-ci sont bien recueillies dans le cadre de procédures judiciaires. Dans le cas contraire, elle pourra enjoindre au ministre de l'intérieur de procéder à la suppression de toute donnée traitée de manière illégale et le sanctionner. Par ailleurs, cette pratique de la police et de la gendarmerie étant installées sur le long terme, la CNIL pourra utilement enjoindre au ministre de l'intérieur d'y mettre fin sans délai.

II. Sur l'illégalité de l'accès au TAJ

A. En ce qui concerne le cadre juridique

47. **En droit**, l'article R. 40-28 du code de procédure pénale prévoit qu'ont accès au TAJ « *pour les besoins des enquêtes judiciaires* » une liste exhaustive d'agents de service de la police nationale et des militaires des unités de la gendarmerie nationale qui ont tous en commun d'exercer « *des missions de police judiciaire* ». Peuvent également être destinataires des données du TAJ d'autres personnes dont des « *agents de l'Etat investis par la loi d'attributions de police judiciaire* ».

9. Vidéo postée sur Twitter et accessible sur https://twitter.com/josly_ngoma/status/1572089719496003586

10. Vidéo postée sur Twitter et accessible sur https://twitter.com/TaoualitAmar/status/1568578798848819209

48. Aussi l'article R. 40-29 du même code prévoit-il l'accès au TAJ pour des catégories d'agents de la police nationale et de la gendarmerie, des agents du service de renseignement, des agents de police administrative pour des situations limitativement énumérées [11], qui correspondent aux enquêtes administrative et au contrôle de grands évènements.

49. Comme il a été énoncé précédemment, le 2° de l'article 4 de la loi Informatique et Libertés prévoit que les données doivent être « *collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités* ». Ce principe doit être interprété à la lumière de la jurisprudence précitée de la CEDH et de la CJUE. Dès lors, l'accès aux données doit également être mis en œuvre de façon restrictive, en application de ces principe de proportionnalité et de stricte nécessité.

50. Ainsi, pour la CJUE, « *s'agissant de l'accès d'une autorité à des données à caractère personnel, une réglementation ne saurait se limiter à exiger que l'accès des autorités aux données réponde à la finalité poursuivie par cette réglementation, mais elle doit également prévoir les conditions matérielles et procédurales régissant cette utilisation*» (*cf.* CJUE, 6 octobre 2020, *Privacy International*, aff. C-623/17, pt. 77 et jurisprudence citée).

51. En outre, « *dès lors qu'un accès général à toutes les données conservées, en l'absence de tout lien, même indirect, avec le but poursuivi, ne peut être considéré comme étant limité au strict nécessaire, une réglementation nationale régissant l'accès aux données relatives au trafic et aux données de localisation doit se fonder sur des critères objectifs pour définir les circonstances et les conditions dans lesquelles doit être accordé aux autorités nationales compétentes l'accès aux données en cause* » (*cf.* CJUE, gr. ch., 21 décembre 2016, *Tele2 Sverige AB et Tom Watson e. a.*, préc., pt. 119 et jurisprudence citée).

52. L'accès aux données ne saurait ainsi « *être accordé, en relation avec l'objectif de lutte contre la criminalité, qu'aux données de personnes soupçonnées de projeter, de commettre ou d'avoir commis une infraction grave ou encore d'être impliquées d'une manière ou d'une autre dans une telle infraction* » (même arrêt,

11. Enquêtes prévues à l'article 17-1 de la loi n° 95-73 du 21 janvier 1995, aux articles L. 114-1, L. 114-2, L. 211-11-1, L. 234-1 et L. 234-2 du code de la sécurité intérieure, et à l'article L. 4123-9-1 du code de la défense.

pt. 119).

53. Le droit des données personnelles exige donc que l'accès aux données par la police ou la gendarmerie réponde à une logique de proportionnalité, ce qui signifie que les finalités du traitement doivent être interprétées de manière restrictive, de sorte que l'accès ne soit accordé que s'il permet de remplir concrètement l'objectif poursuivi. En outre, l'accès aux données ne doit pas être général mais avoir un lien direct, et recherché pour chaque accès, avec la finalité pour laquelle le traitement est autorisé.

B. En ce qui concerne les illégalités constatées

54. **En troisième lieu**, la mise en œuvre du TAJ est illégale en ce que, en pratique, les personnes habilitées à accéder à ce traitement ne consultent pas les données uniquement pour les finalités de constatation des infractions et de recherche des auteurs dans le cadre des procédures judiciaires.

55. En effet, l'accès à ce fichier est une pratique généralisée et usuelle au sein de la police et la gendarmerie. Un rapport sénatorial fait état de 15 341 000 consultations du TAJ en 2021 [12]. Ce chiffre anormalement élevé révèle une pratique de consultation massive et totalement disproportionnée de ce fichier par les personnes qui y sont habilitées.

56. En outre, l'accès à ce fichier n'est pas limité à des procédures judiciaires réalisées sous le contrôle de l'autorité judiciaire, mais est utilisé de façon massive par les services du ministère de l'intérieur et en tout état de cause dans le cadre de procédures administratives.

57. Parmi elles, l'utilisation de ce système à des fins de simple contrôle d'identité par un ensemble très étendu d'agents, loin de l'affirmation selon laquelle ce dispositif ne serait utilisé que par des « *enquêteurs spécialisés* », a été documentée à plusieurs reprises.

12. Marc-Philippe Daubresse, Arnaud de Belenet et Jérôme Durain, *Rapport d'information sur la reconnaissance faciale et ses risques au regard de la protection des libertés individuelles*, 10 mai 2022, note de bas de page n° 3 p. 38, URL : `https://www.senat.fr/rap/r21-627/r21-6271.pdf`

58. C'est notamment ce qu'a été révélé le ministre de l'intérieur lui-même lors d'une séance au Sénat du 16 mars 2021 portant sur la proposition de loi dite « sécurité globale » [13] :

> « *J'en viens à la façon de procéder au contrôle d'identité.*
>
> *Lorsqu'une personne n'a pas de pièce d'identité et que l'on n'est pas en mesure de vérifier son identité, il faut alors faire un acte relevant de la police d'enquête, de la police judiciaire : recours au TAJ, qui est un fichier de police judiciaire, ou réalisation de recherches pour vérifier l'identité de la personne.*
>
> *Ces recherches sont parfois très compliquées. La personne concernée peut, par exemple, être un étranger en situation irrégulière qui n'a plus aucun papier et dont l'administration française essaie de savoir depuis de nombreuses années qui il est, où il est né, de quel pays il vient, dans quelles conditions il est venu en France. Il peut aussi s'agir d'un Français ayant, pour diverses raisons, usurpé une identité. Il y a 850 000 usurpations d'identité par an dans notre pays !* »

59. Comme il sera démontré ci-après, l'utilisation du TAJ dans le cadre de contrôle de police administrative est principalement utilisé à travers les dispositifs de reconnaissance faciale.

60. Ainsi, le ministre de l'intérieur a révélé publiquement une pratique visant à utiliser une procédure judiciaire permettant d'accéder au TAJ alors qu'aucun délit n'est commis, induisant un accès disproportionné à ce fichier.

61. En outre, l'accès au TAJ par d'autres acteurs, et notamment les services de renseignement, est également censé être limité au strict nécessaire. Or, l'article R. 40-29 qui autorise cet accès exceptionnel ne prévoit aucune garantie permettant de restreindre ledit accès à certaines catégories de personnes, à un certain nombre d'utilisation, à certains types de données ou encore de prévoir une base légale pour que la CNIL puisse contrôler cette consultation du fichier.

13. Compte-rendu intégral de la séance du mardi 16 mars 2021 du Sénat, p. 41, URL : `https://www.senat.fr/seances/s202103/s20210316/s20210316.pdf`

62. Le rapport d'information sur les fichiers mis à la disposition des forces de sécurité précité affirme d'ailleurs que « *les services de renseignement spécialisés, ainsi que les services concourant à la mission de renseignement peuvent, dans le cadre des besoins liés à la protection de certains intérêts, consulter* ***le fichier TAJ****. Cette consultation s'opère selon un profil spécifique permettant d'accéder à toutes les données des procédures judiciaires, y compris celles concernant des procédures en cours.* » [14]

63. En pratique, l'accès par les services de renseignement au TAJ n'est pas limité au strict nécessaire et outrepasse les quelques limites posées par l'article R. 40-29 du code de procédure pénale, les services de renseignement pouvant accéder à toutes les données des procédures judiciaires. Au demeurant, la Commission nationale de contrôle des techniques de renseignement (CNCTR) n'est investie d'aucun pouvoir pour contrôler les modalités de consultation du TAJ par les services de renseignement, ce qui permet en pratique un fort risque d'abus et d'arbitraire. Il revient donc à la CNIL d'exercer les prérogatives qui lui sont confiées au titre de l'article 19 de la loi Informatique et Libertés pour vérifier la légalité de cet accès.

64. **En conclusion**, la mise en œuvre par ministre de l'intérieur du TAJ viole délibérément la loi Informatique et Libertés en ne limitant pas au strict nécessaire l'accès au traitement et en autorisant sa consultation dans des situations qui ne sont pas prévues par les dispositions du code de procédure pénale.

III. Sur l'accès au TAJ par reconnaissance faciale

A. En ce qui concerne le cadre juridique

1. S'agissant du code de procédure pénale

65. **En droit**, l'alinéa 16 de l'article R. 40-26 du code de procédure pénale, tel que créé par le décret n° 2012-652 du 4 mai 2012, prévoit que peut être enregistrée dans le TAJ la « *photographie comportant des caractéristiques techniques permettant de recourir à un dispositif de reconnaissance faciale (photographie du visage*

14. En gras dans le texte.

de face)» concernant les personnes mises en causes et les personnes faisant l'objet d'une enquête ou d'une instruction pour recherche des causes de la mort ou d'une disparition.

66. D'après l'avis rendu par la CNIL dans sa délibération n° 2011-204 du 7 juillet 2011, cette disposition permettrait notamment de « *comparer à la base des photographies signalétiques du traitement, les images du visage de personnes impliquées dans la commission d'infractions captées via des dispositifs de vidéoprotection* ».

2. S'agissant du droit des données personnelles

67. Aux termes de l'article 10 de la directive « police-justice » :

> « *« Le traitement des* [...] *données biométriques aux fins d'identifier une personne physique de manière unique* [...] *est autorisé uniquement en cas de nécessité absolue, sous réserve de garanties appropriées pour les droits et libertés de la personne concernée, et uniquement :*
>
> *a) lorsqu'ils sont autorisés par le droit de l'Union ou le droit d'un État membre ;*
>
> *b) pour protéger les intérêts vitaux de la personne concernée ou d'une autre personne physique ; ou*
>
> *c) lorsque le traitement porte sur des données manifestement rendues publiques par la personne concernée.* »

68. Ce principe d'interdiction de traiter des données biométriques a été transposé à l'article 6 de la loi Informatique et Libertés et se retrouve également à l'article 9 du RGPD.

69. L'article 8 de la Charte prévoit que « *Toute personne a droit à la protection des données à caractère personnel la concernant* » et que « *Ces données doivent être traitées loyalement, à des fins déterminées et sur la base du consentement de la*

personne concernée ou en vertu d'un autre fondement légitime prévu par la loi. »

70. Le 1 de l'article 52 de la Charte prévoit que :

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

71. Ces dispositions impliquent que, pour être justifiée, toute atteinte à un droit engendrée par un traitement de données biométriques doit être prévue par la loi (a), ne pas porter atteinte à l'essence de ce droit (b) et être proportionnée au regard de l'objectif poursuivi (c).

a. Nécessité d'une base légale

72. En application de la Charte, pour la CJUE, le droit de l'Union doit « *prévoir des règles claires et précises régissant la portée et l'application de la mesure en cause et imposant un minimum d'exigences de sorte que les personnes dont les données ont été conservées disposent de garanties suffisantes permettant de protéger efficacement leurs données à caractère personnel contre les risques d'abus ainsi que contre tout accès et toute utilisation illicites de ces données* » (cf. CJUE, gr. ch., 8 avril 2014, *Digital Rights Ireland e. a.*, aff. C-293/12 et C-594/12, pt. 54 et jurisprudence citée).

73. Elle ajoute que « *la nécessité de disposer de telles garanties est d'autant plus importante lorsque, comme le prévoit la directive 2006/24, les données à caractère personnel sont soumises à un traitement automatique et qu'il existe un risque important d'accès illicite* à ces données» (même arrêt, pt. 55).

74. Le considérant 33 de la directive « police-justice » dispose que le droit d'un

État membre « *devrait être clair et précis et son application devrait être prévisible pour les justiciables, conformément à la jurisprudence de la Cour de justice et de la Cour européenne des droits de l'homme. Le droit des États membres qui réglemente le traitement des données à caractère personnel relevant du champ d'application de la présente directive devrait préciser au minimum les objectifs, les données à caractère personnel qui feront l'objet d'un traitement, les finalités du traitement et les procédures pour garantir l'intégrité et la confidentialité des données à caractère personnel et les procédures prévues pour la destruction de celles-ci, fournissant ainsi des garanties suffisantes vis-à-vis des risques d'utilisation abusive et d'arbitraire.* »

75. En ce qui concerne la CESDH, aux termes de l'article 8 de la CESDH, toute ingérence dans le droit à la vie privée doit être « *prévue par la loi* ».

76. La CEDH a ainsi considéré que l'ingérence devait avoir « *une base en droit interne* », être par ailleurs « *suffisamment accessible* », le citoyen devant « *pouvoir disposer de renseignements suffisants, dans les circonstances de la cause, sur les normes juridiques applicables à un cas donné* » et enfin que ne pouvait être considéré comme une loi au sens de la CESDH « *qu'une norme énoncée avec assez de précision pour permettre au citoyen de régler sa conduite ; en s'entourant au besoin de conseils éclairés, il doit être à même de prévoir, à un degré raisonnable dans les circonstances de la cause, les conséquences de nature à dériver d'un acte déterminé* » (*cf.* CEDH, 25 mars 1983, *Silver et autres c. Royaume-Uni*, n° 5947/72, §§ 85–88).

77. De la même façon, il a été jugé que :

> « *Les mots* "prévue par la loi" *veulent d'abord que la mesure incriminée ait une base en droit interne, mais ils ont trait aussi à la qualité de la loi en cause : ils exigent l'accessibilité de celle-ci à la personne concernée, qui de surcroît doit pouvoir en prévoir les conséquences pour elle, et sa compatibilité avec la prééminence du droit* [...]. *Cette expression implique donc notamment que la législation interne doit user de termes assez clairs pour indiquer à tous de manière suffisante en quelles circonstances et sous quelles conditions elle habilite la puissance publique à recourir à des mesures affectant leurs droits protégés*

par la Convention » (*cf.* CEDH, 12 juin 2014, *Fernandez Martinez c. Espagne*, n° 56030/07, § 117)

78. Il a ainsi suffi à la Cour européenne de constater que la mesure incriminée n'était pas prévue par la loi pour conclure à la violation de l'article 8 de la Convention (*cf.* CEDH, 8 avril 2003, *M. M. c. Pays-Bas*, n° 39339/98, §. 46 ; voir dans ce sens également : CEDH, *Guide sur l'article 8 de la Convention - Droit au respect de la vie privée et familiale*, §. 14). Pour la Cour, les risques d'arbitraire sont d'autant plus évidents que la mesure de surveillance est exercée en secret et que les technologies utilisées sont toujours plus sophistiquées (*cf.* CEDH, 21 juin 2011, *Shimovolos c. Russie*, n° 30194/09, § 68).

79. Dans son projet de lignes directrices relatives à l'utilisation de reconnaissance faciale en matière de police et de justice [15], le Comité européen de la protection des données (ci-après le « CEPD ») rappelle que ce principe de prévision de la loi doit être appliqué à la reconnaissance faciale [16].

80. Pour le CEPD, étant donné que les données biométriques, lorsqu'elles sont traitées dans le but d'identifier de manière unique une personne physique, constituent des catégories particulières de données énumérées à l'article 10 de la directive « police-justice », les différentes applications de la reconnaissance faciale nécessitent, dans la plupart des cas, une loi spécifique décrivant précisément l'application et les conditions de son utilisation (*Idem.*, pt. 44). Il est ainsi essentiel que les mesures législatives qui visent à fournir une base juridique à une mesure de reconnaissance faciale soient prévisibles pour les personnes concernées et qu'une telle loi ne peut résulter de la seule transposition de l'article 10 de la directive « police-justice » [17].

15. CEPD, Projet de *lignes directrices 05/2022 relatives à l'utilisation de reconnaissance faciale en matière de police et de justice*, 16 mai 2022, URL : `https://edpb.europa.eu/system/files/2022-05/edpb-guidelines_202205_frtlawenforcement_en_1.pdf`

16. *Idem.*, pt. 52.

17. *Idem.* §§ 70 et 71.

b. Atteinte à l'essence du droit

81. Le considérant 46 de la directive « police-justice » rappelle que « *Toute limitation des droits de la personne concernée doit respecter la Charte et la convention européenne des droits de l'homme, telles qu'elles sont interprétées respectivement par la Cour de justice et par la Cour européenne des droits de l'homme dans leur jurisprudence, et notamment respecter l'essence desdits droits et libertés.* »

82. L'évaluation de ce critère implique d'examiner si le contenu essentiel du droit est respecté, c'est-à-dire si le droit est effectivement vidé de son contenu essentiel. Dès lors qu'il est porté atteinte au contenu essentiel du droit, la mesure est contraire à la Charte et il n'est alors, par hypothèse, pas nécessaire de poursuivre l'évaluation de sa compatibilité avec les autres règles énoncées au 1 de l'article 52 (légitimé de l'objectif poursuivi ; nécessité ; proportionnalité).

83. Le contenu essentiel des droits à la vie privée et au respect des données personnelles garantis par les articles 7 et 8 de la Charte est composé de plusieurs éléments dégagés par la jurisprudence de la CJUE et États membres en application du droit de l'Union, que ce soit des autorités nationales de protection des données ou des juridictions.

84. En exemple notoire, la Cour a reconnu qu'une « *réglementation permettant aux autorités publiques d'accéder de manière généralisée au contenu de communications électroniques doit être considérée comme portant atteinte au contenu essentiel du droit fondamental au respect de la vie privée, tel que garanti par l'article 7 de la Charte* » (*cf.* CJUE, gr. ch., 6 octobre 2015, *Schrems*, aff. C-362/14, pt. 94).

85. Comme le rappelle le CEPD dans ses lignes directrices sur la reconnaissance faciale, la CJUE a également jugé qu'une règle relative à la protection et à la sécurité des données qui ne prévoiraient pas le respect de certains principes de protection et de sécurité des données pouvait également porter atteinte à l'essence du droit à la vie privée [18].

86. Dans la continuité de ce mouvement, concernant la conservation et l'ac-

18. *Idem*., pt. 46 faisant référence au point 40 de l'arrêt *Digital Rights Ireland*.

cès des données de connexion, la CJUE a affirmé que « *le législateur de l'Union a concrétisé les droits consacrés aux articles 7 et 8 de la Charte, de telle sorte que les utilisateurs des moyens de communications 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.* » (*cf.* CJUE, gr. ch., 6 octobre 2020, *La Quadrature du Net e. a.*, préc., pt. 109)

87. Ainsi, pour s'opposer aux techniques de traçage des outils de communication électronique de l'ensemble de la population, la Cour a construit un droit à l'anonymat dans l'espace public auquel elle refuse toute dérogation. Il apparaît ainsi que le contenu essentiel des droits et libertés reconnus aux article 7 et 8 de la Charte comprend un droit à l'anonymat dans l'espace public.

88. Cet arrêt *La Quadrature du Net e. a.* de la CJUE a par ailleurs été appliqué en droit interne des États membres, notamment par la Cour constitutionnelle belge qui, par son contrôle de conventionnalité, a directement appliqué dans l'ordre juridique belge le principe et la conception de l'essence du droit à la vie privée et du droit à la protection des données personnelles (*cf.* Cour constitutionnelle belge, 22 avril 2021, n° 57/2021).

89. La CNIL elle-même soulignait les risques inhérents à la reconnaissance faciale dans une position sur son site Internet en 2019 [19] :

> « *les données extraites des visages touchent au corps, à l'intimité des personnes.* [...] *Dans l'environnement numérique actuel, où les visages des personnes sont disponibles dans de multiples bases de données et captées par de nombreuses caméras, la reconnaissance faciale peut devenir un outil particulièrement omniprésent et intrusif. Le renforcement de la surveillance permis par cette technologie peut enfin réduire l'anonymat dont disposent les citoyens dans l'espace public.* »

19. « Reconnaissance faciale : pour un débat à la hauteur des enjeux », 15 novembre 2019, URL : `https://www.cnil.fr/fr/reconnaissance-faciale-pour-un-debat-la-hauteur-des-enjeux`

c. Exigence de proportionnalité

90. Dans le cadre de la prévention, de la détection, d'enquêtes et de poursuite en matière pénale, l'article 10 de la directive « police-justice » prévoit que « *le traitement* [...] *des données biométriques aux fins d'identifier une personne physique de manière unique* [...] *est autorisé uniquement en cas de nécessité absolue, sous réserve de garanties appropriées pour les droits et libertés de la personne concernée* ». Cette disposition a été transposée à l'article 88 de la loi Informatique et Libertés. Cet article prévoit que le traitement de données dites « sensibles », telles que visées à l'article 6 de cette loi et comprenant les données biométriques, « *est possible uniquement en cas de nécessité absolue, sous réserve de garanties appropriées pour les droits et libertés de la personne concernée* ».

91. Loin d'être une simple formule de style, l'exigence de « nécessite absolue » est une innovation active du législateur. Jusqu'en 2018, les données biométriques n'étaient protégées que par des garanties formelles [20]. Il a fallu attendre la transposition de la directive « police-justice » pour que les données biométriques soient enfin protégées par des garanties substantielles.

92. Proposée en 2012 par la Commission européenne, la version initiale de cette directive ne protégeait pas spécifiquement les données biométriques : il s'agissait de simples données personnelles et il suffisait que leur traitement soit « *nécessaire* » à la finalité poursuivie (article 4 de la proposition de directive). C'est la commission « Libertés civiles » du Parlement européen qui a proposé d'ajouter que le traitement de données biométriques soit « strictement nécessaire » [21].

93. Cet ajout a été confirmé par la séance plénière du Parlement européen le 12 mars 2014. Dans sa position du 8 avril 2016, le Conseil a parachevé cette évolution en exigeant une « *nécessité absolue* ».

94. Dans ses lignes directrices précitées sur la reconnaissance faciale, le CEPD donne des indications pour apprécier ce critère lorsqu'il s'agit de technologie de

20. Un décret pris en Conseil d'État en application de l'article 27 de la loi Informatique et Libertés ou une autorisation de la CNIL en application de l'article 25, selon que le traitement était réalisé ou non pour le compte de l'État.

21. Rapport de la commission LIBE, 22 novembre 2013, URL : `https://www.europarl.europa.eu/doceo/document/A-7-2013-0403_FR.html`

reconnaissance faciale [22] :

> « *Un traitement ne peut être considéré comme "strictement nécessaire" que si l'atteinte à la protection des données à caractère personnel et ses restrictions sont limitées à ce qui est absolument nécessaire. L'ajout du terme "strictement" signifie que le législateur a voulu que le traitement de catégories particulières de données ne puisse avoir lieu que dans des conditions encore plus strictes que les conditions de nécessité. Cette exigence doit être interprétée comme étant indispensable. Elle limite à un minimum absolu la marge d'appréciation laissée à l'autorité répressive dans le cadre du test de nécessité. Conformément à la jurisprudence constante de la CJUE, la condition de "stricte nécessité" est également étroitement liée à l'exigence de critères objectifs afin de définir les circonstances et les conditions dans lesquelles un traitement peut être entrepris, excluant ainsi tout traitement de nature générale ou systématique.* »

95. Le CEPD pointe d'ailleurs les risques pour le droit à la vie privée mais également les autres droits affectées par la perte d'anonymat dans l'espace public induite par la reconnaissance faciale. Il rappelle que l'évaluation de la nécessité et de la proportionnalité doit s'effectuer en fonction de chaque situation et identifier et prendre en compte toutes les incidences sur les autres droits fondamentaux, notamment le droit à la dignité humaine protégé par l'article 1er de la Charte, la liberté de pensée, de conscience et de religion protégées par l'article 10 de la Charte, la liberté d'expression protégée l'article 11 de la Charte ainsi que la liberté de réunion et d'association protégée par l'article 12 de la Charte [23].

96. Dans la conclusion des lignes directrices, le CEPD insiste [24] :

> « *Certains cas d'utilisation des technologies de reconnaissance faciale présentent des risques inacceptables pour les individus et la société ("lignes rouges") Pour ces raisons, le CEPD et l'EDPS ont appelé à*

22. CEPD, Projet de *lignes directrices 05/2022 relatives à l'utilisation de reconnaissance faciale en matière de police et de justice*, 16 mai 2022, préc., pt. 73, traduction libre.
23. *Idem*., pt. 58.
24. *Idem*., pt. 104, traduction libre.

leur interdiction générale [...] *En outre, le CEPD considère que le traitement des données personnelles dans un contexte répressif qui s'appuierait sur une base de données alimentée par la collecte de données personnelles à grande échelle et de manière indiscriminée, par exemple en "aspirant" des photographies et des images faciales accessibles en ligne, en particulier celles mises à disposition via les réseaux sociaux, ne répondrait pas, en tant que tel, à l'exigence de stricte nécessité prévue par le droit de l'Union.* »

97. Comme cela a été évoqué ci-avant, dans le cadre d'un avis conjoint portant sur la proposition de règlement relatif à « l'intelligence artificielle », l'EDPS et le CEPD ont demandé une « *interdiction générale de toute utilisation de l'IA en vue d'une reconnaissance automatisée des caractéristiques humaines dans des espaces accessibles au public, tels que les visages, mais aussi la démarche, les empreintes digitales, l'ADN, la voix, la pression sur des touches et d'autres signaux biométriques ou comportementaux, dans tous les contextes.* » Cette demande d'interdiction repose sur le constat que « *compte tenu de la directive [« police-justice »], du RPDUE et du RGPD, l'EDPB et le CEPD ne peuvent discerner comment ce type de pratique serait en mesure de satisfaire aux exigences de nécessité et de proportionnalité, deux notions qui découlent en définitive de ce qui est considéré comme acceptable par la CJUE et la Cour européenne des droits de l'homme* » [25].

98. Au sein des autres États membres, la question de la conformité au droit de l'Union d'un dispositif de reconnaissance faciale policier se pose également de manière de plus en plus importante.

99. Ainsi, dans un avis de 2021 [26], aux visas notamment de la directive « police-justice », de l'article 8 de la CESDH, et des articles 7, 8 et 52 de la Charte, l'autorité italienne de protection des données a estimé que le système de la police italienne de reconnaissance faciale « SARI Real Time » n'était pas conforme au droit italien et européen de protection des données, notamment parce qu'il n'était pas pro-

25. Avis conjoint 05/2021 de l'EDPB et du CEPD sur la proposition de règlement du Parlement européen et du Conseil établissant des règles harmonisées concernant l'intelligence artificielle, § 32, URL : `https://edpb.europa.eu/system/files/2021-10/edpb-edps_joint_opinion_ai_regulation_fr.pdf`

26. Avis négatif de l'autorité italienne de protection des données relatif au dispositif de reconnaissance faciale « SARI Real Time », 25 mars 2021, URL : `https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9575877`

portionné. L'autorité relevait notamment que « *le système en question effectue un traitement automatisé à grande échelle qui peut concerner, entre autres, également ceux* [...] *qui ne font pas l'objet "de recherches" par les forces de police.* »

100. De même, l'incompatibilité avec la directive « police-justice » de l'utilisation par une autorité de police des services de l'entreprise Clearview AI, qui offre un dispositif de reconnaissance faciale similaire à celui du TAJ – comme avec le TAJ, les possibilités de traçage de la population sont décuplées, notamment parce que les images issues de la base de données de Clearview AI proviennent des réseaux sociaux et permettent de tirer des conséquences très précises et intimes sur la vie privée des personnes – a déjà été relevée par l'EDPB dans une lettre adressée à des députés européens [27] :

> « *L'EDPB considère que le traitement de données personnelles dans un contexte répressif qui s'appuierait sur une base de données alimentée par la collecte de données personnelles à grande échelle et de manière indiscriminée, sans aucune limitation ni aucun lien précis entre les données collectées et l'objectif poursuivi, serait, en tant que tel, susceptible de ne pas répondre à l'exigence de nécessité absolue prévue par la directive [« police-justice »]* ».

101. C'est ainsi que le 10 février 2021, l'autorité suédoise de protection des données personnelles a sanctionné la police suédoise pour son utilisation du logiciel Clearview AI qui contrevenait au principe de nécessité absolue du droit suédois transposant la directive « police-justice ». L'autorité écrivait notamment que ce dispositif de reconnaissance faciale utilisé par la police suédoise ne « [répondait pas] *à l'exigence de nécessité absolue de la loi* [suédoise] *sur les données criminelles et de la directive* [« police-justice »] » [28]

27. Lettre du CEPD/EDPB datée du 10 juin 2020 à des députés européens concernant la conformité du dispositif Clearview AI au droit de l'UE, traduction libre, URL : `https://edpb.europa.eu/sites/default/files/files/file1/edpb_letter_out_2020-0052_facialrecognition.pdf`

28. Sanction de la police par l'autorité suédoise de protection des données, en raison de l'utilisation du logiciel de reconnaissance faciale de Clearview AI, traduction libre, URL : `https://www.imy.se/globalassets/dokument/beslut/beslut-tillsyn-polismyndigheten-cvai.pdf`

B. En ce qui concerne les faits reprochés

102. À titre liminaire, il convient de rappeler que la pratique de la reconnaissance faciale par le ministre de l'intérieur est parfaitement avérée. Le rapport d'information précité de 2018 fait état des outils utilisés par les services de police et de gendarmerie [29] :

> « *L'outil GASPARD NG permet aussi d'alimenter le TAJ des photographies des mis en cause. Il est ainsi désormais possible de lancer dans le TAJ des recherches à partir d'une photographie. Les résultats de la recherche font apparaître les photographies déjà présentes susceptibles d'y correspondre en fonction d'un certain nombre de paramètres (écartement des yeux, etc.). La recherche peut ailleurs être affinée par certains critères, tels que le sexe, la couleur des yeux ou des cheveux, etc. Le TAJ constitue déjà, de ce point de vue, un outil de reconnaissance faciale.*
>
> [...]
>
> *Le TAJ comporte déjà une fonctionnalité de reconnaissance faciale permettant, dans le cadre d'investigations judiciaires, d'opérer des rapprochements avec les photographies de personnes mises en cause déjà inscrites dans ce fichier. Cette fonctionnalité permet également de proposer des "tapissages" de photos faciales de suspects afin de les soumettre aux victimes.* »

103. Il ne fait pas débat que ces traitements sont des traitements de données biométriques réalisés en matière pénale. D'après ce même rapport, « *le TAJ comprend entre 7 et 8 millions de photos de face* » [30].

104. Dans le rapport d'information sénatorial précité, il est par ailleurs affirmé que [31] :

29. Didier Paris, Pierre Morel-À-L'Huissier, *Rapport d'information sur les fichiers mis à la disposition des forces de sécurité*, 17 octobre 2018, préc.

30. *Idem*., p. 64.

31. Marc-Philippe Daubresse, Arnaud de Belenet et Jérôme Durain, *Rapport d'information sur la reconnaissance faciale et ses risques au regard de la protection des libertés individuelles*, 10 mai 2022, préc., pp. 37–38

« Un dispositif de rapprochement par photographies est opéré dans le ***fichier du « Traitement des antécédents judiciaires » (TAJ)*** *constitué de données recueillies, dans le cadre des procédures établies par les* ***services de sécurité intérieure*** *(police nationale, gendarmerie nationale et douanes). Ce traitement, prévu par les articles R. 40-23 à R. 40-34 du code de procédure pénale, est mis en œuvre par le ministre de l'intérieur (direction générale de la police nationale et direction générale de la gendarmerie nationale) afin de faciliter la constatation des infractions à la loi pénale, le rassemblement des preuves de ces infractions et la recherche de leurs auteurs.*

Depuis 2012, l'article R. 40-26 du code de procédure pénale autorise les forces de sécurité intérieure à ***utiliser la reconnaissance faciale pour identifier les personnes fichées dans le TAJ****. Il s'agit d'un* ***outil d'aide à l'enquête****, qui peut par exemple permettre à un enquêteur qui dispose d'une photographie de l'auteur des faits d'orienter ses recherches vers une personne déjà connue du TAJ. Il est également possible* ***d'établir des liens entre des affaires différentes****, voire de les attribuer à un même auteur sur la base de sa reconnaissance sur les photographies disponibles. Cet outil vient en soutien de l'enquêteur et est paramétré pour donner un maximum de 200 réponses avec un taux de correspondance minimum de 40 %. C'est l'enquêteur qui procède* in fine *à l'identification de la personne.*

*Cette fonctionnalité par "*rapprochement de photo de personne*" est mise en œuvre principalement* ***dans le cadre d'une enquête judiciaire, sous la direction et le contrôle d'un magistrat****. Elle peut également être utilisée dans le cadre du renseignement en application de l'article L. 234-4 du code de la sécurité intérieure qui permet aux agents individuellement désignés et spécialement habilités des services spécialisés de renseignement des ministères de l'intérieur, de la défense, des finances et des comptes publics, de consulter le TAJ, selon un profil spécifique leur permettant d'accéder à toutes les données des procédures judiciaires, y compris celles en cours, à l'exclusion de celles relatives aux victimes.*

L'utilisation de l'outil de reconnaissance faciale pour interroger le TAJ est ***en accroissement notable depuis quelques années****. En 2021, il a été*

> *utilisé 498 871 fois par la police nationale et environ 117 000 fois par la gendarmerie nationale. Selon la direction centrale de la police judiciaire (DCPJ), qui est le gestionnaire du traitement, cette montée en puissance de l'utilisation de l'outil pourrait être consécutive à l'évolution technique de l'outil intervenue en 2019 qui en a nettement amélioré la performance.* »[32]

105. Déjà, dans sa délibération n° 2011-204 du 7 juillet 2011, la CNIL considérait que « *cette fonctionnalité d'identification, voire de localisation, des personnes à partir de l'analyse biométrique de la morphologie de leur visage, présente des risques importants pour les libertés individuelles, notamment dans le contexte actuel de multiplication du nombre des systèmes de vidéoprotection* ». L'évolution des technologies et le constat des pratiques décrites ci-dessus ont radicalement modifié le contexte de l'analyse de ces dispositifs, nécessitant un nouvel examen de l'autorité, particulièrement depuis l'adoption de la directive « police-justice » et du critère de nécessité absolue.

106. Cette analyse devra nécessairement la conduire à conclure que l'utilisation de la reconnaissance faciale par le ministre de l'intérieur est contraire à la Charte des droits fondamentaux et à la loi Informatique et Liberté en ce qu'elle repose sur aucune base légale suffisante (1), porte atteinte à l'essence du droit à la vie privée (2) et, à titre subsidiaire, ne répond à aucun critère de proportionnalité (3).

1. S'agissant de l'absence de base légale

107. **En quatrième lieu**, la mise en œuvre d'un traitement de reconnaissance faciale par le ministre de l'intérieur pour accéder aux données du TAJ n'est pas conforme la Charte, à la directive « police-justice » et à la loi Informatique et Libertés en ce qu'elle manque d'une base légale suffisante.

108. Le ministre de l'intérieur fonde l'utilisation de la reconnaissance faciale par ses agents sur l'article R. 40-26 du code de procédure pénale. Or, si cette disposition mentionne bien cette technologie, ce n'est que pour préciser les paramètres

32. En gras dans le texte.

de collecte des photographie liées aux infractions qu'il convient de constater ou rechercher.

109. En aucun cas il ne s'agit d'une base légale suffisante pour procéder à un traitement de données biométriques, tel que celui permis par la reconnaissance faciale, au sens de la directive « police-justice ».

110. En application de la Charte, dès lors qu'il s'agit d'un traitement spécifique, au surplus sur des données biométriques, qui est une opération différente et plus complexe que la simple consultation du TAJ par des informations nominatives, l'utilisation de la reconnaissance faciale devrait faire l'objet d'une réglementation claire et prévisible permettant de protéger efficacement les personnes concernées contre les risques d'abus et contre tout accès et toute utilisation illicites de leurs données.

111. Or, non seulement le code de procédure pénale ne prévoit ni autorisation de procéder à ces traitements, mais il ne prévoit pas non plus de critères objectifs encadrant cette pratique.

112. **Premièrement**, aucun texte n'encadre la nature des données avec lesquelles les photographies contenues dans le TAJ peuvent être comparées. En pratique, cela permet aujourd'hui d'utiliser des images issues de réseaux sociaux, mais aussi de vidéosurveillance publique ou privée, ou de photographies prises par les policiers eux-mêmes avec leurs téléphones portables, comme cela a été illustré *supra*.

113. **Deuxièmement**, il n'y a pas de finalité spécifique pour lesquelles ces opérations pourraient être effectuées, les finalités prévues par l'article 230-6 du code de procédure pénale étant bien trop générales et larges pour une technologie aussi intrusive que la reconnaissance faciale. De la même manière, il n'existe pas de cadre limitant le nombre de personnes pouvant avoir accès à cette technologie, ou définissant leur habilitation.

114. **Troisièmement**, l'extrait précité du rapport sénatorial de 2022 fait également état d'une utilisation par les services de renseignement de l'outil de reconnaissance faciale alors que cet accès n'est jamais encadré par la loi, ce qui le soustrait

à tout contrôle, d'autant que la CNCTR n'a pas accès au TAJ dans le cadre de ses missions de contrôle.

115. Enfin, **quatrièmement**, il n'existe aucune procédure permettant de garantir l'intégrité et la confidentialité des données personnelles. L'outil de reconnaissance faciale ne répond à aucune condition de transparence ou d'intégrité permettant de savoir dans quelle mesure les données sont traitées et détruites.

116. Déjà, il en résulte que l'article R. 40-26 ne peut être une base légale suffisante pour protéger les droits fondamentaux dans le cadre d'opérations généralisées de reconnaissance faciale par le ministre de l'intérieur, qui sont donc illégales.

2. S'agissant de l'atteinte à l'essence du droit à la vie privée

117. **En cinquième lieu**, la mise en œuvre d'un traitement de reconnaissance faciale par le ministre de l'intérieur pour accéder aux données du TAJ n'est pas conforme la Charte, à la directive « police-justice » et à la loi Informatique et Libertés en ce qu'elle porte atteinte à l'essence des droits fondamentaux protégés au niveau de l'UE.

118. Le traitement de données contesté ne peut se comprendre qu'en se rappelant qu'il réalise un lien entre deux ensembles de données.

119. **Premièrement**, l'État dispose d'un nombre considérable, voire illimité, de sources d'images issues de l'espace public. D'une part, l'essentiel des lieux de vie publics est filmé par les innombrables caméras de vidéosurveillance. En 2020, pour la seule région parisienne, la Cour des comptes estime à 41 000 leur nombre [33]. D'autre part, les autorités peuvent collecter des images sur Internet ou en capturer elle-même, par exemple par drones, hélicoptères, caméras-piétons ou lors de contrôles d'identité, tels qu'illustrés *supra*. Eu égard au contexte de leur captation, ces images donnent des informations très précises sur les agissements ou habitudes des personnes, par exemple lorsque celles-ci sont prises lors d'une manifestation ou sur un réseau social public. Par ce premier mécanisme, les autorités peuvent

33. «*Le plan de vidéoprotection de la préfecture de police de Paris*», 2 décembre 2021, p. 3, URL : `https://www.ccomptes.fr/fr/documents/58747`

connaître le visage associé aux déplacements et aux activités dans l'espace public de potentiellement l'ensemble de la population.

120. **Deuxièmement**, près de 10 millions de personnes identifiées ont déjà une image de leur visage dans le TAJ. La police peut librement compléter ce fichage au cours de ses activités, que ce soit en collectant des images sur Internet ou en les capturant elle-même sur le terrain, tel que cela été démontré. Par ce second mécanisme, les autorités peuvent connaître le visage associé à l'identité de potentiellement l'ensemble de la population.

121. **Troisièmement**, le dispositif de reconnaissance faciale du TAJ permet de faire le lien de façon automatique et massive entre ces deux ensembles de données (les images de l'espace public captées et contextualisées d'une part, et les personnes déjà identifiées dans le TAJ d'autre part). Ainsi, les autorités peuvent connaître l'identité associée aux déplacements et aux activités dans l'espace public de potentiellement l'ensemble de la population. C'est ce lien automatisé et massif entre identité et comportement dans l'espace public qui est contesté, entre autres, par la présente plainte, que la mise en œuvre du TAJ permet. Ce lien crée des atteintes aux droits fondamentaux qui ne se comprennent qu'en ayant à l'esprit les multiples données qui vont être rapprochées de manière automatisée et massive. Le nombre d'opérations de reconnaissance faciale démontre que ce traitement n'est pas ponctuel mais bien généralisé, voire systématique.

122. La situation est très similaire à celle déjà vivement rejetée par la CJUE en matière de conservation généralisée des données de géolocalisation (*cf.* CJUE, gr. ch., 6 octobre 2020, *La Quadrature du Net e. a.*, préc.). Dans les deux cas, les autorités peuvent connaître les déplacements et l'identité de potentiellement toute personne, que cela passe par les données de géolocalisation propres aux outils de communication pour la première situation ou par les données biométriques propres aux individus, dans le cas présent. La situation est même plus grave encore en l'espèce dans la mesure où il est bien plus difficile pour une personne d'altérer ou de dissimuler ses données biométriques que de changer ou de dissimuler ses outils de communication.

123. Par ailleurs, dès lors qu'elle est couplée à un régime de vidéosurveillance généralisée, la fin de l'anonymat dans l'espace public permet aux autorité de prendre connaissance du contenu des activités publiques de potentiellement l'ensemble de

la population, ce qui est une atteinte du même ordre de gravité que la conservation généralisée du contenu des communications électroniques, reconnue explicitement par la Cour comme contraire au contenu essentiel du droit à la vie privée et au respect des données personnel (*cf.* CJUE, gr. ch., 6 octobre 2015, *Schrems*, préc., pt. 9).

124. En outre, le CEPD rappelle dans ses lignes directrices concernant les traitements de reconnaissance faciale que « *le fait qu'une photographie ait été manifestement rendue publique par une personne concernée n'implique pas que les données biométriques correspondantes, qui peuvent être extraites de la photographie par des moyens techniques spécifiques, soient considérées comme ayant été rendues publiques.* » (pt. 74)

125. Dans le cas des réseaux sociaux ou des plateformes en ligne, le CEPD considère que « *le fait que la personne concernée n'ait pas déclenché ou paramétré des fonctions de confidentialité spécifiques n'est pas suffisant pour considérer que cette personne a manifestement rendu publiques ses données à caractère personnel et que ces données (par exemple des photographies) peuvent être transformées en modèles biométriques et utilisées à des fins d'identification sans le consentement de la personne concernée*» (*Idem*., pt. 76)

126. Les risques et dangers engendrés par la reconnaissance faciale doivent donc être analysée au regard de ces éléments et de ce contexte de multiplication des sources d'images – qu'il s'agisse de vidéosurveillance ou des réseaux sociaux – qui empêchent aujourd'hui toute forme d'anonymat dans l'espace public.

127. **Il en résulte que** les pratiques de reconnaissance faciale du ministre de l'intérieur portent atteinte à l'essence du droit à la vie privée et doivent être, à nouveau, considérées comme illégales.

3. S'agissant de l'absence de nécessité absolue

128. **En sixième lieu**, la mise en œuvre d'un traitement de reconnaissance faciale par le ministre de l'intérieur pour accéder aux données du TAJ n'est pas conforme la Charte, à la directive « police-justice » et à la loi Informatique et Li-

bertés en ce qu'elle n'est pas absolument nécessaire à la recherche d'infractions.

129. En effet, la police utilise cet outil lors de simples contrôles d'identités. Cela a été notamment illustré lors d'un reportage diffusé sur la chaîne TF1 le 23 janvier 2020 et intitulé « Les nuits de Marseille » [34] dans lequel un agent de la police nationale effectue une comparaison biométrique lors d'un simple contrôle [35]. Un témoignage au cours d'une opération à Montreuil en février 2021 fait également état du recours à la reconnaissance faciale pour identifier des personnes interpellées [36].

130. L'utilisation du dispositif attaqué à des fins de contrôle d'identité a également été confirmé en février 2022 par un ensemble de messages sur les réseaux sociaux mentionnant une note très récente de la direction générale de la police nationale (DGPN) interdisant l'utilisation du dispositif de reconnaissance faciale « *lors d'une opération de contrôle d'identité prévue à l'article 78-2 du [code de procédure pénale]* » (*cf.* pièce n° 2). Il serait également précisé dans cette note qu'« *Une interrogation du TAJ n'est licite que pour les besoins exclusifs des missions de police administrative ou judiciaire* » (même pièce).

131. L'existence de cette note révèle non seulement que le traitement attaqué n'est pas utilisé dans le seul cas de procédures judiciaires, mais également que la DGPN considère que l'utilisation alors faite par la police nationale du dispositif à des fins de contrôle d'identité n'était pas légale et qu'elle devait être proscrite. La Quadrature du Net a par ailleurs effectué une demande d'accès à cette note en application du livre III du code des relations entre le public et l'administration, demande qui n'a fait l'objet d'un refus implicite malgré l'avis favorable de la Commission d'accès aux documents administratifs (*cf.* pièce n° 3).

132. Un article de juin 2021 publié sur le site d'actualités Gendinfo, édité par la direction générale de la gendarmerie nationale (DGGN), révèle que, concernant

34. URL vers le reportage complet : `https://www.tf1.fr/tf1/sept-a-huit/videos/les-nuits-de-marseille-une-commissaire-a-poigne-05174510.html`

35. URL vers l'extrait : `https://video.lqdn.fr/w/xr4qR4AeBCa3JT3y7EWAjU`

36. Voir Christophe-Cécil Garnier, « *Dans tous les commissariats de France, on utilise la reconnaissance faciale* », StreetPress, 7 avril 2021, URL : `https://www.streetpress.com/sujet/1617723420-tous-commissariats-france-utilise-reconnaissance-faciale-police-gendarmerie-justice-surveillance-zad-squat-libertes-societe` et « *Expulsion + réoccupation + manif = week-end agité du côté du Marbré !*», Paris-Luttes.info, 1er mars 2021, URL : `https://paris-luttes.info/expulsion-reoccupation-manif-week-14797`

le dispositif de comparaison biométrique, « *Depuis le 24 novembre 2020, cette fonctionnalité* [de consultation du TAJ] *est ouverte à l'ensemble des unités. Auparavant, seules les unités de recherches y avaient accès* [37] ».

133. Cette pratique générale est ancienne. Dès 2013, des gendarmes niçois se réjouissaient auprès de Nice-matin : « *un homme ayant perdu la tête a été trouvé dans le jardin d'une propriété et il s'est révélé incapable de donner son nom. Les gendarmes l'ont pris en photo et nous l'ont envoyé. Et "bingo", sa fiche est sortie. Il a pu être identifié, puisqu'il était connu des fichiers* » [38].

134. Dans un courrier daté du 12 février 2020 et adressée à La Quadrature du Net dans le cadre d'une demande d'abrogation (*cf.* pièce n° 4), la ministre de la justice, garde des sceaux, indique que « *le dispositif de reconnaissance faciale constitue une aide technique au rapprochement opéré par l'enquêteur à partir d'éléments d'information obtenus au cours des investigations menées* ». Le rôle de simple « *aide technique* » s'oppose en soi au critère de « nécessité absolue ». En d'autres termes, l'aveu de la seule « utilité » du dispositif démontre l'absence de « nécessité » et, *a fortiori*, l'absence de toute nécessité absolue.

135. Sur ce point, il convient de revenir sur l'appréciation qui a été faite par le Conseil d'État sur ces dispositions. En effet, celui-ci a validé la légalité de l'alinéa 16 de l'article R. 40-26 du code de procédure pénale en estimant que ce dispositif n'était pas disproportionné (Conseil d'État, 26 avril 2022, *La Quadrature du Net*, n° 442364).

136. Déjà, **premièrement**, lorsque le Conseil d'État relève que ce dispositif ne pouvait « *être utilisé par les services compétents qu'en cas de nécessité absolue, appréciée au regard des seules finalités du traitement, lorsque subsiste un doute sur l'identité d'une personne dont l'identification est requise* », il créé un nouveau critère abstrait et large qui ne saurait suffire à limiter l'ingérence dans le droit à la vie privée. En effet, au regard des critères posés par la Charte, et son interprétation par la CJUE et le CEPD, « *le doute sur l'identité d'une personne dont l'identification est requise* » ne saurait constituer une finalité suffisamment précise ni permettre un

37. Antoine Faure, « Au départ de l'enquête», Gendinfo, 31 mai 2021, URL : https://www.gendinfo.fr/dossiers/criminalistique-le-futur-des-a-present/au-depart-de-l-enquete

38. « "TAJ", le logiciel qui reconnaît les délinquants », Nice-Matin, 31 mars 2013, URL : https://www.nicematin.com/faits-societe/taj-le-logiciel-qui-reconnait-les-delinquants-337064

cadre juridique suffisamment clair et protecteur pour limiter les conséquences que la reconnaissance faciale engendre sur les droits et libertés.

137. **Deuxièmement**, le Conseil d'État justifie la nécessité absolue de la reconnaissance faciale de la façon suivante :

> « *Eu égard au nombre de personnes mises en cause enregistrées dans ce traitement, qui s'élève à plusieurs millions, il est matériellement impossible aux agents compétents de procéder manuellement à une telle comparaison, de surcroît avec le même degré de fiabilité que celui qu'offre un algorithme de reconnaissance faciale correctement paramétré. Or une telle identification à partir du visage d'une personne et le rapprochement avec les données enregistrées dans le TAJ peuvent s'avérer absolument nécessaires à la recherche des auteurs d'infractions et à la prévention des atteintes à l'ordre public, toutes deux nécessaires à la sauvegarde de droits et de principes de valeur constitutionnelle*.»

138. Cette interprétation de la nécessité absolue doit être écartée, et ce, à deux égards.

139. **D'une part**, le Conseil d'État apprécie la condition de nécessité absolue non pas au regard de la *finalité* du TAJ mais vis à vis des *moyens utiles* pour que ce traitement soit *lui-même* nécessaire à la recherche d'auteurs infractions. En effet, l'atteinte au droit à la vie privée engendrée par l'accès au TAJ par un dispositif de reconnaissance faciale est justifiée par une nécessité première de remplir un objectif de prévention des atteintes à l'ordre public et de recherche d'auteurs d'infractions. Ce faisant, le Conseil d'État évalue si l'atteinte à la vie privée engendrée par la reconnaissance faciale est nécessaire non pas à remplir l'objectif du traitement (recherche d'auteurs d'infractions et prévention des atteintes à l'ordre public), mais si elle est nécessaire pour accéder efficacement aux données du traitement. En effet, il n'effectue pas de balance vis à vis des droits des personnes concernées mais uniquement au regard du fonctionnement général du TAJ et de son efficacité. Cette interprétation mobilise donc de façon erronée les principes de finalité, de proportionnalité et de nécessité absolue.

140. **D'autre part**, cette interprétation, qui revient à justifier une atteinte aux

droits par l'utilité qu'elle confère à une autre atteinte aux droits est en opposition avec l'esprit de la protection du droit à la vie privée. La CEDH a ainsi sanctionné un raisonnement similaire en estimant que, dans le cadre d'un système de conservation indiscriminée et illimitée des données personnelles, accepter l'argument selon lequel plus les données sont conservées, plus la criminalité serait évitée, reviendrait en pratique à justifier le stockage d'informations sur l'ensemble de la population et de leurs proches décédés, ce qui serait certainement excessif et dénué de pertinence (*cf.* CEDH, 13 février 2020, *Gaughran c. Royaume-Uni*, n° 45245/15, § 89 [39]. De la même manière, ici, c'est la quantité disproportionnée de données contenues dans le TAJ – tel que cela a été démontrée dans le I – qui justifierait pour le Conseil d'État de mettre en place un traitement automatisé et excessif de ces données au moyen de la reconnaissance faciale.

141. Très récemment, la CJUE a également souligné que « *le manque de ressources allouées aux autorités publiques ne saurait en aucun cas constituer un motif légitime permettant de justifier une atteinte aux droits fondamentaux garantis par la Charte* » (*cf.* CJUE, gr. ch., 1er août 2022, *Vyriausioji tarnybinės etikos komisija*, aff. C-184/20, pt. 89). Ainsi, les questions d'ordre matériel ne saurait rentrer dans l'appréciation de la proportionnalité d'une atteinte au droit à la vie privée.

142. **Troisièmement**, pour justifier de la proportionnalité du dispositif, le Conseil d'État estime que « *le traitement litigieux comporte des garanties appropriées pour les droits et libertés des personnes* » dès lors que le TAJ ne serait accessible qu'à une certaine catégorie d'agents et qu'il existerait un contrôle de ce traitement par des magistrats ainsi que par la CNIL.

143. Il a été démontré ci-avant que les conditions fixées par le code de procédure pénale ne garantissent pas, en pratique, une limitation suffisante et conforme aux exigences du droit de l'Union européenne d'accès au fichier par des opérations de reconnaissance faciale. En outre, a également été illustrée l'insuffisance, voire l'inexistence, du contrôle du traitement par les magistrats chargés de le faire. Surtout, ce contrôle n'est pas opéré de façon systématique à chaque accès au traitement par un outil de reconnaissance faciale, ce qui empêche que cet examen de nécessité absolue soit garanti à chaque atteinte aux droits générée par la reconnaissance faciale.

39. Voir plus précisément le point 108 du *Guide sur la jurisprudence de la Convention européenne des droits de l'homme relative aux données personnelles*, 2022.

144. Enfin, le Conseil d'État mentionne l'existence du contrôle que la CNIL peut opérer aux fins de s'assurer du respect, en pratique, des droits des personnes concernées mentionnés à l'article R. 40-33. Tout comme le contrôle des magistrats, celui-ci n'est pas systématique et au regard du nombre d'opérations de reconnaissance faciale chaque année, il ne saurait suffire à pallier l'atteinte portée aux droits des personnes.

145. **Il en résulte que**, la mise en œuvre de la reconnaissance faciale dans le cadre du TAJ par le ministre de l'intérieur n'est pas absolument nécessaire, ni assortie de garanties suffisantes. À nouveau, cette mise en œuvre du TAJ doit être déclarée illégale.

146. À tous égards, une sanction du ministre de l'intérieur pour sa mise en œuvre du TAJ s'impose.

PAR CES MOTIFS, l'association La Quadrature du Net et les 15 248 plaignants l'ayant mandatée concluent qu'il plaise à la CNIL de :

— Sur la collecte de données :

CONTRÔLER la pertinence, l'adéquation et la proportionnalité des données contenues dans le traitement TAJ au regard de ses finalités ;

ENJOINDRE, au ministre de l'intérieur de supprimer les données traitées de manière disproportionnée ou contraire aux conditions fixées par le code de la sécurité intérieure ;

SANCTIONNER, le ministre de l'intérieur pour les violations constatées.

— Sur l'accès au traitement :

CONTRÔLER l'effectivité de la restriction de l'accès au traitement TAJ conformément aux dispositions du code de la sécurité intérieure et du principe de proportionnalité ;

ENJOINDRE, au ministre de l'intérieur de cesser tout accès au traitement TAJ qui ne serait pas conforme aux aux dispositions du code de la sécurité intérieure et au principe de proportionnalité ;

SANCTIONNER, le ministre de l'intérieur pour les violations constatées.

— Sur l'accès au traitement au moyen de la reconnaissance faciale :

CONTRÔLER l'utilisation des outils de reconnaissance faciale faite par le ministre de l'intérieur ;

ENJOINDRE, au ministre de l'intérieur, à titre principal, de cesser tout accès au traitement TAJ par des moyens de reconnaissance faciale en ce que ce traitement n'est pas prévu par la loi et porte atteinte au contenu essentiel du droit à la vie privée et, à titre subsidiaire, dès lors que la reconnaissance faciale n'est jamais absolument nécessaire pour atteindre les finalités du traitement ;

SANCTIONNER, le ministre de l'intérieur pour l'utilisation illégale, durable et manifestement délibérée de cette technologie et les violations constatées.

Fait à Marseille, le 24 septembre 2022

[redacted]

Membre du collège solidaire de La Quadrature du Net

[redacted]

BORDEREAU DES PRODUCTIONS

Pièce n° 1 : Liste des 15 248 plaignants ayant donné mandat à La Quadrature du Net pour déposer en leur nom la présente plainte ;

Pièce n° 2 : Tweets mentionnant l'existence d'une note de la DGPN relative aux conditions d'utilisation du TAJ ;

Pièce n° 3 : Avis n° 20222095 du 12 mai 2022 de la Commission d'accès aux documentas administratifs ;

Pièce n° 4 : Lettre du 12 février 2020 par laquelle Mme Nicole Belloubet, Garde des Sceaux, ministre de la justice, a refusé l'abrogation des dispositions réglementaires du TAJ.