Délibération SAN-2023-017 du 11 décembre 2023

Commission Nationale de l'Informatique et des Libertés

Nature de la délibération : Sanction
Etat juridique : En vigueur

Date de publication sur Légifrance : Mercredi 31 janvier 2024

Délibération de la formation restreinte n°SAN-2023-017 du 11 décembre 2023 concernant le ministère de l'intérieur et des Outre-mer et le ministère de l'Europe et des Affaires étrangères

La Commission nationale de l'informatique et des libertés, réunie en sa formation restreinte composée de M. Alexandre LINDEN, président, M. Philippe-Pierre CABOURDIN, vice-président, MM. Bertrand du MARAIS et Alain DRU, Mmes Christine MAUGÜE et LATOURNARIE-WILLEMS, membres ;

Vu le règlement (CE) no 1987/2006 du Parlement européen et du Conseil du 20 décembre 2006 sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen de deuxième génération (SIS II) ;

Vu le règlement (CE) n o 767/2008 du Parlement européen et du conseil du 9 juillet 2008 concernant le système d'information sur les visas (VIS) et l'échange de données entre les États membres sur les visas de court séjour (règlement VIS) ;

Vu le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des données à caractère personnel et à la libre circulation de ces données ;

Vu le règlement (UE) n° 2018/1861 du Parlement européen et du Conseil du 28 novembre 2018 sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen (SIS) dans le domaine des vérifications aux frontières, modifiant la convention d'application de l'accord de Schengen et modifiant et abrogeant le règlement (CE) no 1987/2006 ;

Vu la loi no 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, notamment ses articles 20 et suivants ;

Vu le décret no 2019-536 du 29 mai 2019 pris pour l'application de la loi no 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ;

Vu l'arrêté du 22 août 2001 portant création d'un traitement informatisé d'informations nominatives relatif à la délivrance des visas dans les postes diplomatiques et consulaires ;

Vu la délibération no 2013-175 du 4 juillet 2013 portant adoption du règlement intérieur de la Commission nationale de l'informatique et des libertés ;

Vu les décisions du 14 août 2020 n° s2020-277C et 2020-278C de la présidente de la Commission nationale de l'informatique et des libertés ;

Vu la décision de la présidente de la Commission nationale de l'informatique et des libertés portant désignation d'un rapporteur devant la formation restreinte, en date du 19 juin 2023 ;

Vu le rapport de Mme Sophie LAMBREMON, commissaire rapporteure, notifié au ministère de l'intérieur et des Outre-mer et au ministère de l'Europe et des Affaires étrangères le 10 juillet 2023 ;

Vu les observations écrites versées par le ministère de l'intérieur et des Outre-mer et le ministère de l'Europe et des Affaires étrangères le 24 aout 2023 ;

Vu les observations orales formulées lors de la séance de la formation restreinte, le 26 octobre 2023 ;

Vu la note en délibéré présentée par le ministère de l'intérieur et des Outre-mer et le ministère de l'Europe et des Affaires étrangères reçue le 13 novembre 2023 ;

Vu les autres pièces du dossier ;

Étaient présents, lors de la séance de la formation restreinte :

- Mme Sophie LAMBREMON, commissaire, entendue en son rapport ;

En qualité de représentants du ministère de l'intérieur et des Outre-mer :

- […]

En qualité de représentants du ministère de l'Europe et des Affaires étrangères :

- […]

Le ministère de l'intérieur et des Outre-mer et le ministère de l'Europe et des Affaires étrangères ayant eu la parole en dernier ;

La formation restreinte a adopté la décision suivante :

I. Faits et procédure

1. Le système d'information sur les visas (VIS) est un système d'information européen qui a pour objectif d'améliorer la mise en œuvre de la politique commune en matière de visas, la coopération consulaire et les consultations des autorités centrales chargées des visas. Il est composé d'un système central, dont la gestion opérationnelle est effectuée par l'agence EU-LISA et d'une infrastructure de communication entre le VIS principal et les interfaces nationales.

2. Le VIS contient des informations relatives aux demandeurs de visa et aux demandes (passées et en cours) qu'ils ont formulées (demandes acceptées, refusées, annulées…). Il est utilisé pour l'examen des demandes de visas de court séjour et des décisions de refus, de prorogation, d'annulation ou de retrait de visa, ainsi que les vérifications des visas et les vérifications et identifications des demandeurs et des détenteurs de visa.

3. En France, le portail Réseau mondial Visas 2 (RMV2), créé par l'arrêté du 22 août 2001 susvisé, permet d'accéder aux données du VIS. Il est composé d'un système central (RMV2 central) et de 157 postes consulaires (RMV2 locaux).

4. L'application informatique RMV 2 permet, lors du dépôt d'une demande de visa, l'interrogation systématique :

- du fichier d'opposition du SIS, en application de la convention d'application de l'accord de Schengen et des règlements (CE) n o 767/2008 puis (UE) n° 2018/1861 susvisés ;

- du VIS en application du règlement (CE) n° 767/2008 susvisé ;

- du fichier d'authentification des actes d'état civil.

5. En application des décisions de la présidente de la Commission nationale de l'informatique et des libertés (la CNIL ou la Commission) n° s2020-277C et 2020-278C en date du 14 août 2020, des délégations de la Commission ont procédé à plusieurs opérations de contrôle sur place et sur pièces. Un contrôle sur pièces a été réalisé et un courrier a été adressé le 11 décembre 2020 au ministère de l'Europe et des Affaires étrangères (MEAE), puis deux contrôles sur place ont été réalisés les 3 et 4 mars 2021 dans les services relevant du MEAE. Ces missions avaient pour objet de procéder à la vérification sur place de la conformité aux dispositions applicables des traitements de données à caractère personnel du SIS II et de tout traitement faisant l'objet d'une interconnexion avec celui-ci mis en œuvre par le MEAE et le ministère de l'intérieur et des Outre-mer (MI) ainsi que des traitements de données à caractère personnel relatifs à la délivrance des visas par les autorités françaises et de tout traitement faisant l'objet d'une interconnexion avec ceux-ci mis en œuvre par le MEAE et le MI.

6. Aux fins d'instruction de ces éléments, la présidente de la Commission a, le 19 juin 2023, désigné Mme Sophie LAMBREMON en qualité de rapporteure, sur le fondement de l'article 22 de la loi du 6 janvier 1978.

7. À l'issue de son instruction, la rapporteure a, le 10 juillet 2023, fait signifier au MI et au MEAE un rapport détaillant les méconnaissances des articles 32 et 34 du règlement 767/2008 et 9 et 12 du règlement 1987/2006 et les manquements aux 1°, 4° et 6° de l'article 4 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 ") qu'elle estimait constitués en l'espèce. La rapporteure proposait à la formation restreinte de prononcer une injonction de mettre en conformité le traitement avec les dispositions des articles 4.1 ; 4.4 et 4.6, de la loi

Informatique et Libertés, 9, 12 et 31 du règlement n°1987/2006 34 et 32 2. i) du règlement n° 2008/767, ainsi qu'un rappel à l'ordre. Elle proposait également que cette décision soit rendue publique et ne permette plus d'identifier nommément les ministères à l'expiration d'un délai de deux ans à compter de sa publication.

8. Le 24 août 2023, les deux ministères ont produit des observations.

9. La rapporteure et les deux ministères ont présenté des observations orales lors de la séance de la formation restreinte.

II. Motifs de la décision

A. Sur la réglementation applicable et les autorités de contrôle

10. Aux termes du 1. de l'article 44 le règlement (CE) no 1987/2006 applicable aux jours des contrôles : " La ou les autorités désignées dans chaque État membre et investies des pouvoirs visés à l'article 28 de la directive 95/46/CE (les "autorités de contrôle nationales") contrôlent en toute indépendance la licéité du traitement des données à caractère personnel dans le cadre du SIS II sur leur territoire et leur transmission à partir de celui-ci, y compris pour ce qui concerne l'échange et le traitement ultérieur d'informations supplémentaires ".

11. Aux termes de l'article 49 du même règlement : " Les États membres veillent à ce que toute utilisation abusive de données introduites dans le SIS II ou tout échange d'informations supplémentaires contraire au présent règlement fasse l'objet de sanctions effectives, proportionnées et dissuasives conformément à leur droit national ".

12. Le 1. de l'article 55 du règlement n° 2018/1861, désormais applicable, dispose que : " Les États membres veillent à ce que les autorités de contrôle indépendantes désignées dans chaque État membre et investies des pouvoirs mentionnés au chapitre VI du règlement (UE) 2016/679 ou au chapitre VI de la directive (UE) 2016/680 contrôlent la licéité du traitement des données à caractère personnel dans le SIS sur leur territoire, leur transmission à partir de leur territoire et l'échange et le traitement ultérieur d'informations supplémentaires sur leur territoire ".

13. Aux termes de l'article 59 du même règlement : " Les États membres veillent à ce que toute utilisation abusive des données du SIS ou tout traitement de ces données ou tout échange d'informations supplémentaires contraire au présent règlement soit punissable conformément au droit national. / Les sanctions prévues sont effectives, proportionnées et dissuasives ".

14. Aux termes de l'article 36 bis du règlement n° 767/2008 : " Les États membres prennent les mesures nécessaires pour que des sanctions, y compris des sanctions administratives et/ou pénales, effectives, proportionnées et dissuasives, conformément au droit national, soient infligées en cas d'utilisation frauduleuse de données introduites dans le VIS ".

15. Aux termes du 2 de l'article 36 bis du même règlement : " Le règlement (UE) 2016/679 s'applique au traitement de données à caractère personnel par les autorités chargées des visas, des frontières, de l'asile et de l'immigration lorsqu'elles accomplissent des missions au titre du présent règlement ".

16. D'une part, le 1° de l''article 4 de la loi Informatique et Libertés prévoit que tout traitement de données à caractère personnel doit être " licite " . D'autre part, l'article 16 de cette loi donne compétence à la formation restreinte de la CNIL pour sanctionner les responsables de traitement ou les sous-traitants qui ne respectent pas les obligations découlant de la loi Informatique et Libertés.

17. Il en résulte que lorsque des dispositions, contenues dans un acte de droit national ou dans un acte de droit dérivé européen, définissent précisément les modalités informatiques par lesquelles un traitement automatisé de données à caractère personnel doit être opéré, en particulier les mesures de sécurité qui doivent être mises en œuvre, la formation restreinte est compétente pour sanctionner le traitement illicite résultant de la méconnaissance de ces dispositions.

18. La formation restreinte est donc compétente en l'espèce pour examiner les manquements aux articles 4.1, 4.4 et 4.6 de la loi Informatique et Libertés qui résulteraient selon la rapporteure de la méconnaissance des dispositions des règlements n° 1987/2006, 767/2008 et n° 2018/1861.

B. Sur les traitements en cause et la qualification de responsable de traitement

19. Aux termes du dernier alinéa de l'article 2 de la loi du 6 janvier 1978 modifiée, " Sauf dispositions contraires, dans le cadre de la présente loi s'appliquent les définitions de l'article 4 du règlement (UE) 2016/679 du 27 avril 2016 ".

20. En vertu de l'article 4, point 7, du règlement 2016/679, le responsable du traitement est " la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement ".

21. Selon l'article 1er de l'arrêté du 22 août 2001 susvisé : " Est autorisée la création d'un traitement automatisé de données à caractère personnel dénommé Réseau mondial Visas 2 (RMV 2), relevant du ministre des affaires étrangères et du ministre chargé de l'immigration ".

22. La formation restreinte relève que la présente procédure porte sur la base centrale du RMV2 du MEAE et les 157 copies de cette base exploitées au sein des postes consulaires.

23. La formation restreinte constate qu'à ce jour, le MI est responsable de la maitrise d'ouvrage du système d'information RMV2. Le MEAE est responsable de la maitrise d'œuvre et il résulte des pièces du dossier que les finalités et moyens de ce traitement doivent aussi répondre aux besoins opérationnels du MEAE. Ce dernier a donc, avec le ministère de l'intérieur et des Outre-mer, un rôle substantiel dans la définition de ces finalités et moyens.

24. La formation restreinte considère que le ministère de l'intérieur et des outre-mer et le ministère de l'Europe et des Affaires étrangères doivent donc être regardés comme responsables de traitement conjoints.

C. Sur les manquements

1. Sur le manquement relatif à la licéité du traitement

25. D'une part, le 1° de l'article 4 la loi Informatique et Libertés dispose que les données à caractère personnel doivent être : " Traitées de manière licite, loyale et, pour les traitements relevant du titre II, transparente au regard de la personne concernée ".

26. Aux termes de l'article 31 du règlement n°1987/2006 dont les dispositions ont été reprises aux 2., 3. 7. de l'article 41 du règlement n° 2018-1861 : " (…) : " 2. Les données ne peuvent être copiées qu'à des fins techniques, pour autant que cette copie soit nécessaire aux autorités visées à l'article 27 pour effectuer une consultation directe. Les dispositions du présent règlement s'appliquent à ces copies. Les signalements émis par un autre État membre ne peuvent être copiés de leur N. SIS II dans d'autres fichiers nationaux de données. / 3. Les copies techniques visées au paragraphe 2 alimentant des bases de données hors ligne ne peuvent être conservées que pour une durée inférieure à 48 heures. Cette durée peut être prolongée dans une situation d'urgence jusqu'à ce que cette situation d'urgence prenne fin. / Nonobstant l'alinéa 1er, les copies techniques alimentant des bases de données hors ligne destinées aux autorités chargées de délivrer les visas ne seront plus autorisées un an après que l'autorité concernée s'est connectée avec succès à l'infrastructure de communication du Système d'information sur les visas, système à établir dans un règlement à venir, concernant le système d'information sur les visas et l'échange de données entre les États membres sur les visas de court séjour, à l'exception des copies faites pour n'être utilisées que dans des situations d'urgence résultant d'une indisponibilité du réseau de plus de vingt-quatre heures. / (…) 7. Toute utilisation de données non conforme aux paragraphes 1 à 6 sera considérée comme détournement de finalité au regard du droit national de chaque État membre ".

27. D'autre part, le 4° de l'article 4 de la loi Informatique et Libertés dispose que les données à caractère personnel doivent être : " 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 ".

28. Aux termes du 2. de l'article 9 du règlement n°1987/2006 dont les dispositions ont été reprises au 2. du règlement n° 2018-1861 : " Si un État membre utilise une copie nationale, il veille, au moyen des services fournis par le CS-SIS, à ce que les données stockées dans la copie nationale soient identiques et compatibles avec la base de données du SIS II au moyen des mises à jour automatiques visées à l'article 4, paragraphe 4 et à ce qu'une consultation de cette copie produise un résultat équivalent à celui d'une consultation dans la base de données du SIS II ".

29. En premier lieu, la rapporteure relève que la délégation de contrôle a constaté que les données de la copie nationale du SIS (N-SIS) sont copiées dans le RMV2 aux fins de gestion des procédures de délivrance de visas et plus particulièrement de la réalisation des contrôles sécuritaires. Il existe ainsi une copie centrale du RMV2 et 157 copies " locales ", dans les postes consulaires. Ces copies intègrent quotidiennement les signalements issus de la copie N.SIS

30. La rapporteure relève que ces copies sont conservées pour une durée supérieure à 48 heures. Il s'agit en effet de bases pérennes qui font uniquement l'objet de mises à jour quotidiennes ou qui, soit mensuellement, soit ponctuellement, sont dupliquées une nouvelle fois, lorsque les disparités constatées sont trop importantes.

31. La rapporteure relève surtout que le recours à des copies techniques est, en tout état de cause, exclu lorsque les autorités concernées, en l'espèce le MEAE et les postes consulaires, sont reliées depuis au moins un an au VIS. En effet, le règlement (CE) 767/2008 concernant le système d'information sur les visas et l'échange de données entre les États membres sur les visas de courts séjours est entré en vigueur le 9 juillet 2008, soit il y a plus de quinze ans. Il prévoit notamment que le VIS est relié aux systèmes nationaux des États membres afin de permettre aux autorités compétentes

des États membres de traiter les données relatives aux demandes de visas et aux visas délivrés, refusés, annulés, retirés ou prorogés.

32. En second lieu et au surplus, la rapporteure relève que les pratiques constatées par la délégation ne permettent pas de garantir une exactitude des données. En effet, le MEAE reçoit une fois par jour, de la part du service des technologies et des systèmes d'information de la sécurité intérieure (STSI²) du MI, l'ensemble des mouvements du fichier N-SIS (création ou suppression – les modifications étant passées comme des suppressions suivies de créations). Ces mouvements sont répertoriés dans un fichier quotidien, contenant la date du jour. L'horodatage du fichier permet de réaliser un contrôle de chronologie des fichiers de mouvements N-SIS. Chaque jour sont reçus environ 2 500 mouvements. Ces mouvements sont intégrés à la base RMV2 centrale. Ce mécanisme de synchronisation engendre plusieurs milliers d'erreurs par mois : à titre d'exemple, 4,7 % des messages en erreur en janvier 2021 et 2,4 % en novembre 2020.

33. La rapporteure relève que quotidiennement, les mouvements sont adressés par le RMV2 central à chacun des 157 postes consulaires afin qu'ils intègrent les mouvements du N-SIS et mettent ainsi à jour leur base RMV2 locale. Toutefois, si un poste consulaire rencontre des problèmes de réseau, la base RMV2 locale ne sera pas synchronisée en temps réel à la suite de l'envoi par le RMV2 central des mouvements. Hebdomadairement, un dénombrement des signalements N-SIS intégrés aux copies locales du RMV2 est effectué afin de le comparer au nombre de signalements N-SIS présents dans le RMV2 central. Toutefois, ni le contenu ni les identifiants des signalements ne sont comparés. De très nombreux écarts sont constatés. À titre exemple, la semaine du 4 septembre 2020, 81,4 % des copies locales comportaient des écarts avec la base N.SIS. Enfin, mensuellement, un contrôle de la cohérence des données est réalisé. La première semaine de chaque mois, un agent procède à l'inventaire des références des signalements d'erreur (liste des numéros de chaque signalement) dans le système RMV2 central. Ces informations sont transmises au STSI² afin qu'il les compare avec la base N-SIS. Un fichier de mouvement, similaire aux fichiers de mouvement quotidien, est ensuite créé par le STSI² et intégré au RMV2 central selon le même mode, afin de synchroniser cette base avec le N-SIS.

34. La rapporteure relève toutefois que les services du MI et du MEAE n'effectuent aucune analyse de la source des incohérences corrigées lors de ces synchronisations. Le RMV2 reçoit les éléments correctifs sous une forme strictement identique à ceux reçus dans le cadre du traitement nominal quotidien. Il est donc impossible de distinguer un flux correctif d'un flux nominal. De plus, dans RMV2, aucun lien entre une demande de visa et une fiche précise n'est mémorisé. Il n'existe pas de possibilité dans RMV2 de déterminer quelles sont les demandes de visa des personnes dont la fiche a fait l'objet d'une correction à la suite de la synchronisation mensuelle.

35. Les ministères indiquent dans leurs observations écrites que le système d'information France-Visas a été déployé dans la totalité du réseau consulaire depuis la fin mai 2023 et qu'il intègre dès sa conception la correction des manquements dans RMV2. La base centrale et les bases locales connexes du SIS dans les postes consulaires ne sont plus utilisées et sont en cours de démantèlement.

36. Les ministères ajoutent que depuis le 17 janvier 2023, aucun contrôle sécuritaire en lien avec la base centrale ou les bases locales du SIS dans RMV2 n'est mené. Les contrôles SIS des dossiers résiduels restant instruits dans RMV2 (dossiers de long terme majoritairement concernant des réunifications de familles de réfugiés) sont assurés par le module consultations sécuritaires de France-Visas.

37. Les ministères précisent que 73 bases RMV2 avaient été supprimées au 14 août 2023, qu'il était prévu que toutes le soient fin septembre 2023 et que les données de la copie de base N-SIS adossées au RMV2 central ont été supprimées en totalité le 21 août 2023.

38. Les ministères ont indiqué, lors de la séance, que le démantèlement de la totalité des bases locales RMV2 s'était achevé le 17 octobre 2023.

39. La formation restreinte relève que les faits constatés par la délégation et les manquements passés relevés par la rapporteure ne sont pas contestés par les ministères, qui se bornent à faire valoir que le remplacement de RMV2 par France-Visas a permis d'y mettre fin.

40. Il ressort de l'ensemble de ces éléments qu'un manquement à l'obligation de traiter les données de manière licite est caractérisé par la méconnaissance de l'interdiction de copie posée par l'article 31 du règlement n°1987/2006. L'utilisation de ces copies engendre, au surplus, un manquement à l'exactitude des données eu égard à la circonstance que les données du RMV2 et de ces copies locales sont discordantes avec les données du N-SIS sans qu'un système d'analyse et de correction des conséquences de ces erreurs ait été mis en place. Un manquement aux 1° et 4° de l'article 4 de la loi Informatique et Libertés est ainsi constitué.

2. Sur les manquements relatifs à l'obligation de sécurité

41. Aux termes de l'article 4.6° de la loi Informatique et Libertés, les données doivent être " traitées de façon à garantir une sécurité appropriée des données à caractère personnel, y compris la protection contre le traitement non autorisé ou illicite

et contre la perte, la destruction ou les dégâts d'origine accidentelle, ou l'accès par des personnes non autorisées, à l'aide de mesures techniques ou organisationnelles appropriées. ".

42. En vertu de l'article 32 du règlement n° 2008/767 du Parlement européen et du Conseil du 9 juillet 2008 : " 1. L'État membre responsable assure la sécurité des données avant et pendant leur transmission à l'interface nationale. Chaque État membre assure la sécurité des données qu'il reçoit du VIS. 2. Chaque État membre adopte, en ce qui concerne son système national, les mesures nécessaires, y compris un plan de sécurité, pour : / (…) b) empêcher l'accès de toute personne non autorisée aux installations nationales dans lesquelles sont effectuées les opérations qui incombent à l'État membre conformément à l'objet du VIS (contrôles à l'entrée de l'installation) ; / c) empêcher que des supports de données soient lus, copiés, modifiés ou effacés par des personnes non autorisées (contrôle des supports de données) ; / d) empêcher l'introduction non autorisée de données et le contrôle, la modification ou l'effacement non autorisés de données à caractère personnel stockées (contrôle du stockage) ; / e) empêcher le traitement non autorisé de données dans le VIS ainsi que toute modification ou tout effacement non autorisés de données traitées dans le VIS (contrôle de la saisie des données) / (…) i) garantir la possibilité de vérifier et d'établir quelles données ont été traitées dans le VIS, à quel moment, par qui et dans quel but (contrôle de l'enregistrement des données) ".

43. Le 1. de l'article 34 du règlement n° 2008/767 dispose que : " 1. Chaque État membre et l'instance gestionnaire établissent des relevés de toutes les opérations de traitement de données effectuées dans le VIS. Ces relevés indiquent: / a) l'objet de l'accès visé à l'article 6, paragraphe 1, et aux articles 15 à 22 ; / b) la date et l'heure ; / c) le type de données transmises conformément aux articles 9 à 14 ; / d) le type de données utilisées à des fins d'interrogation conformément à l'article 15, paragraphe 2, à l'article 17, à l'article 18, paragraphes 1 et 6, à l'article 19, paragraphe 1, à l'article 19 bis, paragraphes 2 et 4, à l'article 20, paragraphe 1, à l'article 21, paragraphe 1, et à l'article 22, paragraphe 1 ; et / e) la dénomination de l'autorité qui a saisi ou extrait les données. / En outre, chaque État membre établit des relevés du personnel dûment autorisé à saisir ou à extraire les données. 1 bis. Pour les opérations énumérées à l'article 17 bis, un relevé de chaque opération de traitement de données effectuée dans le VIS et l'EES est établi conformément au présent article et à l'article 46 du règlement (UE) 2017/2226 ".

44. En vertu de l'article 12 du règlement n°1987/2006, dont les dispositions ont été reprises à l'article 12 du règlement n° 2018/1861 : " (…) 2. Les États membres qui utilisent des copies nationales veillent à ce que tout accès aux données du SIS II et tout échange de ces données soient enregistrés aux fins mentionnées au paragraphe 1. Ceci n'est pas applicable aux traitements visés à l'article 4, paragraphe 4. / 3. Les enregistrements indiquent, en particulier, l'historique des signalements, la date et l'heure de la transmission des données, les données utilisées pour effectuer une consultation, la référence des données transmises et le nom de l'autorité compétente et de la personne responsable du traitement des données. / 4. Les enregistrements ne peuvent être utilisés qu'aux fins prévues aux paragraphes 1 et 2 et sont effacés au plus tôt après une période d'un an et au plus tard après une période de trois ans suivant leur création. Les enregistrements contenant l'historique des signalements sont effacés après une période d'un à trois ans suivant la suppression des signalements. / 5. Les enregistrements peuvent être conservés plus longtemps s'ils sont nécessaires à une procédure de contrôle déjà engagée (…) "

45. Il résulte de l'ensemble de ces dispositions que les responsables de traitement sont tenus d'apporter un soin particulier à la sécurité des traitements en cause, qui sont particulièrement sensibles, et qu'en particulier la mise en place d'un dispositif de journalisation précis est obligatoire.

46. En premier lieu, la rapporteure relève que la délégation a constaté qu'aucune journalisation des accès n'était mise en œuvre au sein du RMV2. Seules les actions suivantes sont tracées, outre le nom de l'agent ayant réalisé l'action : introduction de la demande de visa, renseignement de la décision prise concernant une demande de visa, signature de la vignette du visa et impression de la vignette du visa. Les actions tracées ne permettent pas d'établir un relevé complet conforme aux exigences des articles 32 2. i) et 34 du règlement n° 2008/767.

47. La rapporteure relève qu'en outre, aucune journalisation des accès à la copie locale du N.SIS n'est mise en œuvre au sein de RMV2, alors même que les agents ayant accès à la copie locale RMV2 depuis un poste consulaire ont la possibilité de réaliser des recherches de signalements N-SIS dans celle-ci.

48. Les ministères indiquent dans leurs observations écrites que l'application France-Visas prend désormais en compte ces obligations de journalisation des accès notamment au sein de la future base de consultation des archives Visas qui se substituera au RMV2 central.

49. Les ministères ajoutent que les droits d'accès sont référencés dans une base de données et maintenus par l'administrateur du module concerné. Celui-ci dispose d'une interface de gestion de droits différenciés en fonction du profil attribué à l'utilisateur. Toute action effectuée au sein du module Instruction est conservée au sein d'une base de données permettant d'identifier chaque modification effectuée sur un dossier (identification du compte et horodatage).

50. La formation restreinte relève que les faits constatés par la délégation de contrôle et les manquements retenus par la rapporteure en matière de journalisation des accès en ce qui concerne le système RMV2 ne sont pas contestés par les ministères, qui se bornent à faire valoir que l'application France-Visas permet de satisfaire aux obligations de journalisation des accès posées par le règlement n°1987/2006.

51. Dès lors, la formation restreinte considère que les actions tracées au sein de l'application RMV2 ne permettent pas d'établir un relevé complet conforme aux exigences des articles 32 2.i) et 34 du règlement n°2008/767 et méconnaissent les exigences des articles précités, ce qui constitue un manquement à l'article.4.6° de la loi Informatique et Libertés.

52. En second lieu, la rapporteure relève que la délégation de contrôle a constaté que […]. Toutefois, les disques durs des postes fixes ne sont pas chiffrés.

53. Eu égard à la sensibilité des données traitées, dans un contexte régalien, la rapporteure estime que le chiffrement des postes utilisateurs de RMV2 constitue une mesure nécessaire à la sécurisation des données, pour le respect de l'article 32 du règlement n° 2008/767.

54. Les ministères indiquent […]

55. En outre, les ministères ont fait valoir, lors de la séance, que le système France-Visas est un système à diffusion restreinte dont il n'est pas possible d'extraire les données sans accès. Un éventuel vol ou une copie de disque dur seraient sans incidence puisqu'ils ne donneraient accès à aucune des données de France-Visas.

56. La formation restreinte relève, en ce qui concerne le système RMV2, que les mesures de restriction des accès évoquées par les ministères répondent aux exigences prévues par l'article 32-2-b) du règlement n° 2008/767contrôles à l'entrée de l'installation), alors que les mesures de chiffrement permettent de répondre aux exigences prévues par l'article 32-2-c) (contrôle des supports de données).

57. La formation restreinte relève que l'application RMV2 […]

58. […]

59. Dès lors, la formation restreinte considère que l'absence de chiffrement des postes fixes […] méconnait les exigences de l'article 32 du règlement n° 2008/767 et constitue un manquement à l'article.4.6° de la loi Informatique et Libertés.

60. Il ressort de l'ensemble de ces éléments que, d'une part, que les ministères n'ont pas respecté les articles 32 2. i) et 34 du règlement n° 2008/767 et 12 du règlement n°1987/2006,et que, d'autre part, l'absence de chiffrement des postes fixes méconnait les exigences du 2 c) de l'article 32 du règlement n° 2008/767, de sorte que les manquements à l'article.4.6° de la loi Informatique et Libertés sont caractérisés.

III. Sur les mesures correctrices et leur publicité

61. Aux termes du III de l'article 20 de la loi du 6 janvier 1978 :

" Lorsque le responsable de traitement ou son sous-traitant ne respecte pas les obligations résultant du règlement (UE) 2016/679 du 27 avril 2016 ou de la présente loi, le président de la Commission nationale de l'informatique et des libertés peut également, le cas échéant après lui avoir adressé l'avertissement prévu au I du présent article ou, le cas échéant en complément d'une mise en demeure prévue au II, saisir la formation restreinte de la commission en vue du prononcé, après procédure contradictoire, de l'une ou de plusieurs des mesures suivantes :

1° Un rappel à l'ordre ;

2° Une injonction de mettre en conformité le traitement avec les obligations résultant du règlement (UE) 2016/679 du 27 avril 2016 ou de la présente loi ou de satisfaire aux demandes présentées par la personne concernée en vue d'exercer ses droits, qui peut être assortie, sauf dans des cas où le traitement est mis en œuvre par l'État, d'une astreinte dont le montant ne peut excéder 100 000 € par jour de retard à compter de la date fixée par la formation restreinte (…) ".

62. La rapporteure propose le prononcé d'un rappel à l'ordre et d'une injonction de mettre le traitement en conformité avec les dispositions la loi Informatique et Libertés s'agissant du manquement à la sécurité des données issu de l'absence de chiffrement des postes fixes des utilisateurs de France-Visas. Elle propose également que cette décision soit rendue publique.

63. En défense, les ministères estiment que le démantèlement du système RMV2 entamé le 17 janvier 2023 et totalement achevé le 17 octobre 2023 est de nature à remédier aux manquements relevés. Ils considèrent que désormais les dispositions relatives à l'obligation de traiter de manière licite et à l'exactitude des données sont pleinement respectées

par le système d'information France-Visas et le décommissionnement du RMV2, qui sont de nature à mettre fin aux manquements relevés, rendant ainsi sans objet un rappel à l'ordre et une injonction de mise en conformité.

64. La formation restreinte, à défaut de pouvoir prononcer une amende administrative, le traitement étant mis en œuvre par l'Etat, considère que les manquements précités justifient le prononcé d'un rappel à l'ordre à l'encontre du MI et du MEAE pour les motifs suivants.

65. La formation restreinte relève que les ministères, hormis le chiffrement des postes fixes, ne contestent pas que les manquements soient constitués pour le passé en ce qui concerne le système RMV2.

66. La formation restreinte relève également qu'un très grand nombre de personnes ont été concernées par le traitement RMV2. La France a reçu 4,3 millions de demandes de visas en 2019, dont 270 000 demandes de visas long séjour.

67. Enfin, la formation restreinte rappelle que les ministères étaient conscients de certains des manquements relevés par le rapport de sanction et qu'ils n'ont pourtant engagé les moyens nécessaires à une mise en conformité à la législation à la protection des données à caractère personnel que très tardivement, le contrôle de la délégation de la CNIL ayant débuté en août 2020. A cet égard, les contraintes budgétaires pesant sur les ministères ne peuvent constituer une justification.

68. La formation restreinte relève que la substitution du système RMV2 par France-Visas ayant mis fin aux manquements constatés dans RMV2, le prononcé d'une injonction de mise en conformité n'apparait plus nécessaire.

69. Enfin, la formation restreinte considère que la publicité de la présente décision se justifie au regard de la gravité des manquements en cause, de la portée du traitement et du nombre de personnes concernées.

70. Elle relève également que cette mesure permettra d'informer les personnes concernées de l'existence du traitement mis en œuvre par les ministères.

71. Enfin, elle estime que cette mesure est proportionnée dès lors que la décision n'identifiera plus nommément les ministères à l'expiration d'un délai de deux ans à compter de sa publication.

PAR CES MOTIFS

La formation restreinte de la CNIL, après en avoir délibéré, décide de :

• prononcer, pour manquements aux articles 4.1, 4.4 et 4.6 de la loi n° 78-17 du 6 janvier 1978 modifiée,

- un rappel à l'ordre à l'encontre du ministère de l'Intérieur et des Outre-mer ;

- un rappel à l'ordre à l'encontre du ministère de l'Europe et des Affaires étrangères ;

• rendre publique, sur le site de la CNIL et sur le site de Légifrance, sa délibération, qui n'identifiera plus nommément les ministères à l'expiration d'un délai de deux ans à compter de sa publication.

Le président

Alexandre LINDEN

Cette décision est susceptible de faire l'objet d'un recours devant le Conseil d'État dans un délai de deux mois à compter de sa notification.