Commission nationale de l'informatique et des libertés

Délibération n° 2022-027 du 3 mars 2022 portant avis sur un projet de décret en Conseil d'Etat fixant les modalités de certification de moyens d'identification électronique ainsi que le cahier des charges permettant d'établir la présomption de fiabilité de ces moyens et un projet de référentiel d'exigences de sécurité pour les moyens d'identification électronique (demande d'avis n° 21021824)

NOR : *CNIX2220911X*

La Commission nationale de l'informatique et des libertés,

Saisie par l'Agence nationale de la sécurité des systèmes d'information d'une demande d'avis concernant un projet de décret en Conseil d'Etat fixant les modalités de certification de moyens d'identification électronique ainsi que le cahier des charges permettant d'établir la présomption de fiabilité de ces moyens et un projet de référentiel d'exigences de sécurité pour les moyens d'identification électronique ;

Vu le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données ou RGPD) ;

Vu la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, notamment son article 32 ;

Sur la proposition de M. Claude CASTELLUCCIA, commissaire, et après avoir entendu les observations de M. Benjamin TOUZANNE, commissaire du Gouvernement,

Emet l'avis suivant :

La Commission a été saisie par l'Agence nationale de la sécurité des systèmes d'information (ANSSI) le 9 décembre 2021 d'une demande d'avis portant sur un projet de décret en Conseil d'Etat fixant les modalités de certification de moyens d'identification électronique ainsi que le cahier des charges permettant d'établir la présomption de fiabilité de ces moyens et un projet de référentiel d'exigences de sécurité pour les moyens d'identification électronique.

La Commission avait été saisie en 2018 par l'ANSSI d'un premier projet de décret fixant le cahier des charges du moyen d'identification électronique et d'un premier projet de référentiel définissant les exigences de sécurité associées au moyen d'identification électronique. Elle a rendu deux avis distincts à ce sujet le 17 janvier 2019 : délibérations n° 2019-005 et n° 2019-006. La Commission relève que ces projets n'ont pas été publiés. Elle prend acte des précisions apportées par l'ANSSI selon lesquelles les présents projets de décret et de référentiel s'inscrivent dans la lignée de la précédente saisine à laquelle ils apportent quelques modifications.

La Commission accueille favorablement la prise en compte par l'ANSSI de la plupart des observations formulées en 2019, notamment au sujet du principe de minimisation des données à caractère personnel et de la possibilité pour les personnes concernées d'exercer leurs droits.

La Commission rappelle qu'en matière d'identification électronique, le règlement (UE) 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 susvisé, dit « règlement e-IDAS », fixe un cadre de référence à l'échelle européenne. Elle rappelle également que la loi n° 2016-1321 pour une République numérique, puis l'ordonnance n° 2017-1426 relative à l'identification électronique et aux services de confiance pour les transactions électroniques, ont élaboré un régime juridique national de l'identité numérique, lequel figure désormais dans le code des postes et des communications électroniques (CPCE).

Dans un premier temps, l'article L. 102 du CPCE prévoit que la preuve de l'identité aux fins d'accéder à un service de communication en ligne peut être apportée par un moyen d'identification électronique. Cet article énonce en outre que ce moyen d'identification est présumé fiable jusqu'à preuve du contraire lorsqu'il répond aux prescriptions du cahier des charges établi par l'ANSSI. La Commission relève que, dans ce contexte, le projet de décret qui lui est soumis pour avis fixe le contenu du cahier des charges précité et établit, au niveau « élevé » au sens du règlement e-IDAS, le niveau de garantie qu'un moyen d'identification électronique doit avoir pour être présumé fiable. Le projet de décret précise également le périmètre (niveaux « substantiel » et « élevé ») et les processus de certification (de la délivrance à l'abrogation) des moyens d'identification électronique prévus par le CPCE en son article L. 102.

Dans un deuxième temps, le projet de référentiel soumis pour avis à la Commission précise les exigences du règlement d'exécution (UE) 2015/1502 du 8 septembre 2015 fixant les spécifications techniques et procédures minimales relatives aux trois niveaux de garantie des moyens d'identification électroniques visés à l'article 8, paragraphe 3, du règlement e-IDAS (« faible », « substantiel » et « élevé »).

Ces éléments généraux rappelés, les projets de décret et de référentiel transmis appellent les observations suivantes.

A titre liminaire, la Commission prend note que le référentiel d'exigence rappelle que tout moyen d'identification électronique suppose un traitement de données à caractère personnel au sens de l'article 4-2 du

RGPD et que la mise en œuvre d'un tel moyen d'identification doit, par sa conception et par défaut, respecter les principes essentiels en matière de protection des données à caractère personnel.

Sur les données traitées :

La Commission prend acte de l'engagement de l'ANSSI à préciser que des précautions particulières doivent être prises pour le traitement des données des personnes sous tutelle, dont le cas a été ajouté au projet de référentiel. Elle accueille favorablement cette précision, ainsi que la nécessité de réaliser une analyse d'impact relative à la protection des données à caractère personnel (AIPD) dans ce cas.

S'agissant de la vérification de l'identité lors de l'enrôlement, le présent projet de référentiel indique que celle-ci peut se faire en face à face physique ou à distance. Dans ce second cas, le projet de référentiel fait référence au référentiel de l'ANSSI applicable aux prestataires de vérification de l'identité à distance (dit « PVID »).

Les exigences relatives à la sécurisation du traitement des données biométriques sont limitées à celles détaillées dans le référentiel PVID pour les seuls prestataires de vérification à distance et à une obligation de sécurisation d'ordre général. Dans ce contexte, la Commission considère que les exigences décrites dans le référentiel PVID pourraient être appliquées à tous les prestataires amenés à traiter ces données.

La Commission rappelle que l'article 9-1 du RGPD pose un principe d'interdiction du traitement de certaines catégories de données dites « sensibles », parmi lesquelles figurent les données biométriques. L'article 9-2 du RGPD précise quant à lui que l'interdiction précitée peut être écartée dans certains cas, notamment lorsque (a) « *la personne concernée a donné son consentement explicite au traitement de ces données à caractère personnel pour une ou plusieurs finalités spécifiques* » ou (g) lorsque le traitement est « *nécessaire pour des motifs d'intérêt public importants* ». La Commission prend acte de l'engagement de l'ANSSI de préciser dans le référentiel que si un traitement de données biométriques du demandeur est réalisé, il doit être justifié par le respect de l'une des conditions prévues à l'article 9.2 du RGPD.

Enfin, la Commission prend note de l'engagement de l'ANSSI à faire apparaitre explicitement l'interdiction de conservation d'empreintes digitales et l'exigence, pour le stockage d'image ou de copie complète de document d'identité, de mettre en œuvre des mesures garantissant un haut niveau de confidentialité.

Sur les droits des personnes :

La Commission relève que l'ANSSI s'engage à ce que le projet de référentiel prévoit que l'utilisateur du moyen d'identification électronique devra disposer « *de l'ensemble des droits prévus par l'article 15, 16, 17, 18, 20 et 21 du [RGPD], sous réserve d'incompatibilité avec les autres exigences applicables au titre du présent référentiel (par exemple, l'exercice par l'utilisateur de son droit de rectification ou de suppression ne doit pas affecter les données archivées pour des raisons de résolution des litiges).* ».

La Commission prend acte des précisions apportées par l'ANSSI relatives au droit à la rectification de données d'identité. Notamment il est précisé que lorsqu'une telle demande est formulée, l'ancienne identité ne sera pas corrigée dans l'archive enregistrée préalablement à cette demande mais que cette demande de correction sera archivée. Elle souhaite que les précisions apportées par l'ANSSI au sujet de l'exercice du droit de rectification soient intégrées au projet de référentiel.

Sur les durées de conservation des données :

La Commission relève que s'agissant des durées de conservation des données à caractère personnel contenues dans tous les types de moyens d'identification électronique, le projet de référentiel prévoit que les informations, en particulier celles utilisées aux fins de la non-répudiation, seront conservées pour une durée de *« six ans à compter de la dernière utilisation pour les moyens d'identification électronique visant le niveau de garantie substantiel ou élevé »*, ou d'*« un an à compter de la dernière utilisation pour les moyens d'identification électronique visant le niveau de garantie faible »*. Le référentiel précise par ailleurs que les informations seront détruites lors du processus de renouvellement ou de remplacement du moyen d'identification électronique, ce qui assure que seul le dernier dossier de preuve relatif à l'individu soit conservé.

La Commission comprend que cette formulation allonge le délai de conservation des données pour les moyens d'identification électronique de niveau substantiel et élevé, délai qui pourrait aller jusqu'à onze ans à compter de la délivrance du moyen d'identification électronique dans l'éventualité où le dossier de preuve serait créé dès l'édition du moyen d'identification électronique.

Si la Commission entend qu'une durée de conservation longue soit nécessaire, elle reste réservée sur la proportionnalité d'une telle durée de conservation des données à caractère personnel. Elle relève notamment que pour la journalisation de données dans des cas similaires, une durée de conservation de 3 ans après les faits avait pu être observée.

Sur les mesures de sécurité :

La Commission rappelle que, s'agissant des traitements pouvant être susceptibles d'engendrer un risque élevé pour les droits et libertés des personnes physiques, une AIPD doit être réalisée et, le cas échéant, lui être transmise si un risque résiduel élevé est identifié à l'issue de l'AIPD, conformément à l'article 36 du RGPD. A cet égard, elle souhaite que la rédaction du paragraphe afférant au sein du projet de référentiel soit modifiée en ce sens.

La présidente,
M.-L. Denis