Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral de justice et police DFJP
Office fédéral de la justice OFJ

Berne, juin 2022

Loi fédérale sur l'identité électronique et d'autres moyens de preuve électroniques

(Loi sur l'e-ID, LeID)

Rapport explicatif pour l'ouverture de la procédure de consultation

Table des matières

Condensé

La numérisation de la société avance à grands pas. La possibilité de s'identifier est un pilier important de cette transformation. Le présent avant-projet de loi vise à introduire une identité électronique (e-ID) étatique pour les titulaires d'un document d'identité émis par les autorités suisses, qui fonctionnera dans une infrastructure gérée par la Confédération. Cette infrastructure permettra de créer et de gérer des moyens de preuve électroniques les plus diverses permettant ainsi d'augmenter leur diffusion et leur utilisation, tout en suivant les développements européens et internationaux et en respectant les exigences de la protection des données personnelles.

Contexte

Le 7 mars 2021, la loi fédérale sur les services d'identification électroniques (LSIE)[1] a été clairement rejetée par presque 65 % des votants. Le 10 mars 2021, six motions de même teneur signées par des représentants de tous les groupes parlementaires ont été déposées au cours de la session de printemps des Chambres fédérales pour demander une e-ID gérée par l'État et digne de confiance (21.3124, 21.3125, 21.3126, 21.3127, 21.3128 et 21.3129).

Le Conseil fédéral a chargé le Département fédéral de justice et police (DFJP), le 26 mai 2021, de s'atteler rapidement à l'ébauche d'une solution d'identification électronique étatique en collaboration avec le Département fédéral des finances (DFF) et la Chancellerie fédérale (ChF). Dans une première étape, le DFJP a préparé un document de travail en association avec des spécialistes des cantons et des experts scientifiques. Cet état des lieux présente trois possibilités techniques de réalisation. Il détaille aussi, notamment, les modalités d'intégration de chacune d'elles dans les échanges économiques et sociaux, ainsi qu'une série d'exemples d'utilisation d'une e-ID étatique.

Le document de travail a fait l'objet d'une consultation publique informelle du 2 septembre au 14 octobre 2021. Soixante avis ont été soumis par des particuliers, des administrations cantonales ainsi que des représentants des milieux scientifiques, des organisations économiques et des entreprises. Pour clôturer la consultation, le DFJP a organisé le 14 octobre 2021 un débat public sous forme de conférence, rassemblant 50 représentants des cantons, des partis politiques, des milieux scientifiques, de la société civile et de l'économie, ainsi que des particuliers intéressés.

Les participants à la consultation se sont exprimés en faveur de l'approche de l'identité auto-souveraine (*Self-Sovereign Identity, SSI*). Ils ont également considéré qu'une infrastructure de confiance complète permettant l'émission et l'utilisation de divers moyens de preuve électroniques. Il s'agit de l'approche qui tient compte des demandes faites par les motions adoptées par le Conseil national le 14 septembre 2021 et par le Conseil des États le 13 juin 2022. Dans le cadre de futurs travaux, il convient de tenir compte de cette volonté ainsi que des principes du respect de la vie privée dès la conception (privacy by design), de l'économie et de l'enregistrement décentralisé des données. En outre, le DFJP souhaite collaborer plus étroitement avec les offices et les cantons qui mènent des projets pilotes connexes en la matière.

Le 17 décembre 2021, le Conseil fédéral s'est fondé sur les résultats de cette consultation et a pris une décision de principe dans laquelle il a jeté les bases de la future e-ID, sous la forme d'un moyen de preuve d'identité électronique émis par l'État.

Les titulaires de l'e-ID devront, dans toute la mesure du possible, avoir la maîtrise de leurs données (principe de l'identité auto-souveraine). La protection des données sera assurée notamment par le système lui-même (principe de la protection de la vie privée dès la conception), mais aussi par la limitation des flux de données nécessaires (principe de l'économie des données) et une sauvegarde décentralisée des données.

L'e-ID fonctionnera dans une infrastructure gérée par l'État, qui pourra, en sus de l'e-ID, être mise à la disposition des services publics et des entreprises pour créer les moyens de preuve électroniques les plus divers, par exemple des extraits du casier judiciaire, des permis de conduire, des diplômes universitaires ou des certificats médicaux. Cet écosystème de moyens de preuves électroniques pourra être élargi progressivement.

Contenu du projet

L'avant-projet de loi prévoit la mise en place d'une identité électronique étatique pour les titulaires d'un document d'identité émis par les autorités suisses. Dans ce cadre, l'État vérifie l'identité d'une personne requérante et lui émet une identité électronique. Le nouveau projet poursuit une approche fondée sur les principes du respect de la vie privée dès la conception (privacy by design), de l'économie et de l'enregistrement décentralisé des données. L'obtention et l'utilisation de l'e-ID demeure volontaire.

En outre, l'avant-projet de loi vise à créer une infrastructure de confiance étatique étendue qui permettra aux acteurs des secteurs public et privé d'émettre et d'utiliser des moyens de preuve électroniques aux personnes intéressées. Dans ce cadre, l'État offrira un portefeuille électronique étatique, qui pourra contenir l'e-ID et d'autres moyens de preuve électroniques. Les titulaires du portefeuille pourront demander, obtenir et présenter leur e-ID ou autres moyens de preuve électroniques de manière sécurisée et transparente. Une telle ouverture du système permettra d'assurer une meilleure diffusion et une utilisation plus fréquente des moyens de preuve électroniques. L'avant-projet de loi tient compte des règles internationales, et en particulier du règlement no 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE. Il prévoit aussi une compétence du Conseil fédéral pour conclure des accords internationaux afin d'obtenir une reconnaissance internationale de l'e-ID et une reconnaissance en Suisse des e-ID étrangères.

[1] FF **2019** 6227

Rapport explicatif

1 Contexte

Le 7 mars 2021, la loi fédérale sur les services d'identification électronique a été rejetée aux urnes par 64 % des votants. Le 10 mars 2021, six motions de même teneur intitulées « À l'État de mettre en place une identification électronique fiable » (cf. 21.3124, 21.3125, 21.3126, 21.3127, 21.3128 et 21.3129) ont été déposées par tous les groupes parlementaires. En outre, l'interpellation 21.3310 Andrey « Coupler l'e-ID avec la carte d'identité » et l'interpellation 21.3718 Graf-Litscher « Identités électroniques souveraines » ont été déposées dans les trois mois suivant la votation. Les six motions ont été adopté le 14 septembre 2021 au premier conseil et la discussion relative à l'interpellation 21.3310 Andrey a été reportée. Le Conseil national a toutefois décidé de liquider l'interpellation 21.3718 Graf-Litscher.

Lors de sa séance du 26 mai 2021, le Conseil fédéral a décidé de recommander au Parlement d'approuver les six motions. En outre, il a déclaré qu'il souhaitait présenter rapidement une nouvelle solution pour l'identification électronique, qui tienne compte des préoccupations des auteurs de la motion. Le Conseil fédéral a ainsi chargé le DFJP d'élaborer, d'ici à la fin de l'année, un concept de base en collaboration avec le Département fédéral des finances (DFF) et la Chancellerie fédérale (CF) et en lien étroit avec les cantons et les deux Écoles polytechniques fédérales de Zurich et Lausanne. Il s'agit en particulier d'examiner les différentes possibilités techniques de réalisation de l'e-ID et de préciser leurs coûts respectifs.

Le DFJP a préparé le « Document de travail concernant le projet d'identité électronique (e-ID) » (ci-après le « document de travail ») en association avec les cantons et des experts scientifiques. Cet état des lieux propose différentes définitions de l'e-ID et de l'infrastructure de confiance y afférente. Il présente également trois approches techniques de réalisation : l'identité souveraine (Self-Sovereign Identity, SSI), l'infrastructure à clé publique (PKI) et le fournisseur d'identité central publique (IdP). Il détaille aussi, notamment, les modalités d'intégration de chacune d'elles dans les échanges économiques et sociaux, ainsi qu'une série d'exemples d'utilisation d'une e-ID étatique.

Le document de travail a fait l'objet d'une consultation publique informelle du 2 septembre au 14 octobre 2021. Soixante avis ont été soumis par des administrations cantonales ainsi que des représentants des milieux scientifiques, des organisations économiques et des entreprises. Pour clôturer la consultation, le DFJP a organisé le 14 octobre 2021 un débat public sous forme de conférence, rassemblant 50 représentants des cantons, des partis politiques, des milieux scientifiques, de la société civile et de l'économie, ainsi que des particuliers intéressés. L'objectif de la consultation publique informelle a été de recueillir des avis sur les principales exigences auxquelles devrait répondre l'e-ID, ses principaux domaines d'utilisation et les avantages attendus. En outre, il s'agissait de connaître l'avis des personnes intéressées sur la portée de l'écosystème e-ID. Les informations récoltées ont permis au Conseil fédéral de prendre une décision de principe concernant la nouvelle orientation de l'e-ID.

Les participants à la consultation se sont exprimés en faveur de l'approche Self-Sovereign Identity (SSI). Ils ont également considéré qu'une infrastructure de confiance avec un niveau d'ambition 3 (cf. document de travail, ch. 4.2) était requise. Il s'agit de l'approche qui tient compte des demandes faites par les motions adoptées par le Conseil national le 14 septembre 2021 et par le Conseil des États le 13 juin 2022. Dans le cadre de futurs travaux, il convient de tenir compte de cette volonté ainsi que des principes du respect de la vie privée dès la conception (*privacy by design*), de l'économie des données et de l'enregistrement décentralisé des données. En outre, le DFJP souhaite collaborer plus étroitement avec les offices et les cantons qui mènent des projets pilotes connexes en la matière.

Se fondant sur les résultats de la consultation publique informelle, le Conseil fédéral a pris une décision de principe le 17 décembre 2021 concernant la nouvelle orientation de l'e-ID. Il a décidé que le projet e-ID poursuivra une approche fondée sur les principes du respect de la vie privée dès la conception (privacy by design), de l'économie des données et de l'enregistrement décentralisé des données ainsi que sur une infrastructure de confiance étatique permettant de mettre en place un écosystème de moyens de preuve électroniques émis par les acteurs des secteurs public et privé. Le Conseil fédéral a prolongé d'un mois le délai de soumission de l'avant-projet de loi destiné à une consultation externe. Finalement, le DFJP s'est vu déléguer la responsabilité, en collaboration avec le DFF (Administration numérique suisse ANS) et la ChF (Secteur Transformation numérique et gouvernance de l'informatique TNI), d'assurer le flux d'information et de coordonner les dépendances entre l'avant-projet de loi et les projets connexes de la Confédération et des cantons.

1.1 Relation avec le programme de la législature et avec les stratégies nationales du Conseil fédéral

L'avant-projet de la loi fédérale sur les moyens d'identification électronique reconnus (loi e-ID, LSIE) a été annoncé dans le message du 27 janvier 2016 sur le programme de la législature 2015 à 2019[2] et dans l'arrêté fédéral du 14 juin 2016 sur le programme de la législature 2015 à 2019[3]. Suite au rejet de ce projet lors de la votation du 7 mars 2021, le Conseil fédéral a décidé de relancer et de réorienter les travaux législatifs en matière d'identité électronique. Le présent avant-projet n'a été annoncé ni dans le message du 29 janvier 2020 sur le programme de la législature 2019 à 2023[4], ni dans l'arrêté fédéral du 21 septembre 2020 sur le programme de législature du 2019 au 2023[5].

2 FF **2016** 981
3 FF **2016** 4999
4 FF **2020** 1709
5 FF **2020** 8087

1.2 Classement d'interventions parlementaires

L'avant-projet de loi proposé met en œuvre les interventions parlementaires suivantes:

- Motions de tous les groupes parlementaires 21.3124, 21.3125, 21.3126, 21.3127, 21.3128 et 21.3129 « À l'État de mettre en place une identification électronique fiable ». Les motions demandent que l'État mette en place un système qui permette de prouver son identité en ligne, de la même manière que la carte d'identité ou le passeport permettent de le faire dans le monde réel. Il doit respecter certains principes : prendre en compte la protection de la vie privée dès la conception du produit (privacy by design), ne collecter que les données nécessaires et enregistrer celles-ci de manière décentralisée (par exemple auprès de l'utilisateur en ce qui concerne les données d'identification). Elle a été acceptée le 14 septembre 2021 par le Conseil national, conformément à la proposition du Conseil fédéral. Elles n'ont pas encore été délibérées au deuxième conseil.

Lors de son élaboration, les interventions parlementaires suivantes ont également été prises en compte:

- Interpellation Andrey 21.3310 « Coupler l'e-ID avec la carte d'identité ». Le 26 mai 2021, le Conseil fédéral a répondu aux questions de l'interpellation. La discussion a été reportée car les réponses n'étaient pas satisfaisantes.

- Interpellation Graf-Litscher 21.3718 « Identités électroniques souveraines ». Le Conseil fédéral a répondu le 18 août 2021 aux questions. Le 1 octobre 2021, le Conseil national a décidé de liquider l'interpellation.

2 Comparaison avec le droit étranger, notamment européen

Des réformes dans le domaine de l'identification électronique sont en cours au sein de l'Union européenne. Le Conseil fédéral estime nécessaire de tenir compte de ces développements dans la réflexion menée au plan national. Le 3 juin 2021, la Commission européenne a adopté une proposition[6] visant à modifier le règlement (UE) no 910/2014 (règlement eIDAS)[7] et à établir un cadre juridique pour une identité électronique européenne. Dans le cadre du nouveau règlement, les États membres offriront aux citoyens et aux entreprises, dans les 12 mois suivant l'entrée en vigueur, des portefeuilles électroniques qui seront en mesure d'établir un lien entre leur identité électronique nationale et la preuve d'autres attributs personnels (tels que permis de conduire, diplômes, compte bancaire). Ces portefeuilles pourront être fournis par des autorités publiques ou par des entités privées, à condition d'être reconnus par les États membres. Au niveau du Parlement, un débat au sein de la commission responsable (ITRE) est prévu pour la fin juin 2022. Le vote en commission est prévu pour octobre 2022 et le vote en plénière en novembre 2022.

Afin que cette initiative se concrétise dans les meilleurs délais, la proposition est accompagnée d'une recommandation. La Commission a invité les États membres à mettre en place une boîte à outils commune d'ici à octobre 2022 et à entamer immédiatement les travaux préparatoires nécessaires. Cette boîte à outils comprendra l'architecture technique, des normes et des lignes directrices relatives aux bonnes pratiques.

Le cadre défini par la Commission repose sur les principes de l'identité autonome (Self-Sovereign Identity, SSI). Pour ce qui concerne la manière précise de mettre en œuvre ces principes, il est cependant technologiquement neutre. Les États membres négocient eux-mêmes les normes techniques depuis septembre 2021.

La Suisse n'a pas d'obligation juridique d'adopter le règlement de l'UE et les modifications qui s'y rapportent. Toutefois, compte tenu de l'étroitesse des rapports commerciaux et sociaux qu'elle entretient avec la plupart des pays membres de l'Union européenne, la Suisse a tout intérêt à rendre son système d'identité électronique interopérable avec celui de l'Union européenne. L'avant-projet de loi prévoit que le Conseil fédéral pourra conclure des accords internationaux afin d'obtenir une reconnaissance internationale de l'e-ID et de reconnaître les e-ID étrangères (art. 25). Il sera ainsi possible d'obtenir à l'avenir une reconnaissance mutuelle, notamment avec l'UE. À ce titre, la reconnaissance du niveau de garantie visé pour l'e-ID étatique suisse est au minimum de niveau de garantie substantiel. L'avant-projet de loi a été formulé de manière à être compatible avec le droit européen en la matière.

3 Grandes lignes du projet

3.1 Nouvelle règlementation proposée

L'avant-projet de loi prévoit la mise en place d'une identité électronique étatique gratuite et volontaire pour les titulaires d'un document d'identité émis par les autorités suisses. Dans ce cadre, l'État continue d'assumer sa tâche centrale, qui est la vérification de l'identité d'une personne ainsi que l'émission du moyen de preuve électronique s'y rapportant. Tel que demandé par les motions soumises au Conseil national, le nouveau projet poursuit une approche fondée sur les principes du respect de la vie privée dès la conception (*privacy by design*), de l'économie des données et de l'enregistrement décentralisé des données.

En outre, l'avant-projet de loi vise à créer une infrastructure de confiance étatique qui permettra aux acteurs des secteurs public et privé d'émettre et d'utiliser des moyens de preuve électroniques. Dans ce cadre, l'État exploitera les systèmes

6 Proposition de Règlement du Parlement Européen et du Conseil modifiant le règlement (UE) no. 910/2014 en ce qui concerne l'établissement d'un cadre européen relatif à l'identité numérique, COM (2021) 281 final, 3 juin 2021.

7 Règlement (UE) no 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE, JO L 257 du 28.8.2014, p. 73.

de base nécessaires (registre de base, système de confirmation des identifiants[8]) et offrira un portefeuille électronique étatique, qui pourra contenir l'e-ID et d'autres moyens de preuve électroniques. Les titulaires du portefeuille pourront présenter leur e-ID et autres moyens de preuve électroniques de manière sécurisée et transparente. Une telle ouverture du système permettra d'améliorer la diffusion et d'augmenter l'utilisation des moyens de preuve électroniques. En même temps, elle permettra de renforcer le niveau de confiance dont bénéficient les processus électroniques au sein de la population.

La mise en place par l'État d'une infrastructure électronique de confiance est un développement important et nouveau. En outre, ce projet se fonde sur une procédure participative novatrice comprenant une consultation informelle, des discussions publiques et un forum de discussion spécialisé en ligne. Il intègre aussi l'expérience acquise dans le cadre des projets pilotes avec d'autres offices et des échanges avec d'autres pays.

La question d'utilisation de l'e-ID dans divers domaines n'est réglée qu'à titre indicatif dans l'avant-projet de loi (cf. modification d'autres actes législatifs : LP et LDEP). La possibilité de l'utiliser dans d'autres domaines sera examinée lors de la consultation externe.

3.2 Adéquation des moyens requis

Les questions relatives à l'adéquation des moyens requis seront analysées en détail à l'issue de la consultation. Une estimation initiale des coûts a été réalisée (cf. ch. 5.1 Conséquences sur les finances et l'état du personnel pour la Confédération).

3.3 Mise en œuvre

Les dispositions d'exécution requises pour la mise en œuvre de la présente loi seront réglées par voie d'ordonnance (cf. art. 27 et les commentaires s'y rapportant).

4 Commentaire des dispositions

Préambule

L'avant-projet de loi se fonde sur les art. 38, al. 1, 81, et 121, al. 1 de la Constitution.

S'agissant de l'identité électronique étatique, l'avant-projet de loi repose sur l'art. 38, al. 1 et l'art. 121, al. 1 Cst. L'art. 38 al. 1 donne la compétence à la Confédération de régler l'acquisition et la perte de la nationalité et des droits de cité par filiation, par mariage ou par adoption. En outre, l'art. 121 al. 1 Cst confère la compétence à la Confédération de légiférer en matière d'entrée en Suisse, de sortie, de séjour et d'établissement des étrangers et d'octroi de l'asile. Bien que ces deux articles ne règlent pas expressément les documents d'identité, il va de soi que la Confédération ait la compétence de régler les documents d'identité requis, même si ceux-ci ne servent pas exclusivement à prouver la nationalité des citoyens suisses et le statut de séjour des étrangers. Se fondant sur ces deux articles, la loi sur les documents d'identité[9] et loi du 16 décembre 2005 sur les étrangers et l'intégration (LEI)[10] permettent à la Confédération d'émettre des documents d'identité aux citoyens suisses et des permis aux étrangers. Comme l'e-ID étatique sert à prouver l'identité dans le monde virtuel, il est donc justifié de fonder le présent avant-projet de loi sur les mêmes bases constitutionnelles pour ce qui concerne les preuves officielles de l'identité, de nationalité et du statut des étrangers.

La compétence de créer une infrastructure de confiance autour de l'e-ID se fonde sur l'art. 81 Cst, qui permet à la Confédération de réaliser, dans l'intérêt du pays ou d'une grande partie de celui-ci, des travaux publics, d'exploiter elle-même des ouvrages publics ou d'encourager leur réalisation. L'encouragement à l'exploitation et à l'entretien d'ouvrages de tiers ne peut en revanche pas se fonder sur l'art. 81; il pourrait tout au plus se fonder sur une compétence fédérale. Un « ouvrage » ou des « travaux publics » visés par cette cette disposition sont traditionnellement de nature physique, au sens d'une construction, comme par exemple un tunnel. Toutefois, selon l'avis de droit de l'OFJ concernant la coopération TIC entre la Confédération et les cantons[11], il serait possible, selon une approche partiellement soutenue par la doctrine, d'inclure dans la notion « travaux » de l'art. 81 Cst les grands projets informatiques et autres éléments visant à créer un paysage administratif électronique uniforme[12]. En effet, suivant l'interprétation évolutive et téléologique de Lendi[13] et de Biaggini[14], les « travaux publics » peuvent également être immatériels ou non tangibles, tels un système informatique ou un système de communication réalisé dans l'intérêt de la Suisse. Le Conseil fédéral se rallie à ce courant doctrinal; il considère donc qu'il est admissible de fonder sur l'art. 81 un avant-projet de loi qui vise à mettre en place une infrastructure de confiance permettant d'émettre, d'utiliser et de valider divers moyens de preuve électroniques (y compris l'e-ID). Dans ce cadre, il convient de rappeler que l'art. 81 Cst ne confère pas à la Confédération de compétence d'édicter et d'imposer

8 Selon l'art. 18, al. 2, la Conseil fédéral peut prévoir que la Confédération confirme aussi les identifiants et les clés cryptographiques des émetteurs et vérificateurs privés.
9 RS **143.1**
10 RS **142.20**
11 EJPD, Bundesamt für Justiz, Rechtsgrundlagen für die IKT-Zusammenarbeit zwischen dem Bund und den Kantonen, Gutachten vom 22. Dezember 2011, JAAC 2012.1 (p. 1 - 17), édition du 1er mai 2012.
12 Ibid, p. 8 : «Zusammengefasst wäre es nach einem in der Lehre teilweise befürworteten Ansatz möglich, grössere Informatikvorhaben und andere Elemente zur Schaffung einer einheitlichen elektronischen Verwaltungslandschaft unter dem Werkbegriff von Art. 81 BV zu subsumieren».
13 Ibid; Lendi, Martin, in St. Galler Kommentar, 2e éd. 2008, art. 81 N. 6
14 Ibid; Biaggini, Giovanni in BV-Kommentar, Zürich 2007, art. 81 N 2, critiqué par Markus Kern im Basler Kommentar, N 6 et 9.

des normes techniques et organisationnelles contraignantes pour une collaboration TIC entre la Confédération et les cantons.[15]

Le présent avant-projet de loi règle certains aspects de droit civil relatifs aux relations entre les émetteurs et les titulaires d'une e-ID ainsi que les vérificateurs et les titulaires d'une e-ID. Cependant, étant donné leur importance accessoire, le préambule ne cite pas l'art. 122, al. 1, Cst, qui établit la compétence de la Confédération en matière de droit civil.

Section 1 Objet et but

Art. 1

Al. 1

L'avant-projet de loi établit le cadre juridique des moyens de preuve électroniques en Suisse, y compris l'identité électronique étatique. Il règle également les exigences relatives à l'infrastructure de confiance servant à l'émission, la révocation, le contrôle, la conservation et la présentation des moyens de preuve électroniques. En outre, l'avant-projet de loi règle les rôles et les compétences prévues dans le cadre de l'exploitation de l'infrastructure de confiance.

Al. 2

Let. a

L'avant-projet de loi vise à mettre en place une identité électronique (e-ID) étatique sûre qui pourra être utilisée entre personnes privées et auprès des autorités publiques. L'e-ID permettra aux titulaires de s'identifier plus facilement dans le cadre des transactions exécutées dans le monde numérique. Elle permettra ainsi de remplacer les processus d'identification (en ligne) existants qui sont beaucoup plus complexes. Pouvant être téléchargée sur un smartphone, l'e-ID pourra également être utilisée dans le monde réel.

Let. b.

La protection des données devant être préservée, la présente lettre reprend le but fixé à l'art. 1 de la loi du 25 septembre 2020 sur la protection des données (nLPD)[16]. Elle rappelle que le traitement des données personnelles effectué dans le cadre de l'obtention et de l'utilisation de l'e-ID respecte les exigences de la protection des données. Ce but sera notamment atteint par la mise en œuvre des exigences des six motions de même teneur intitulées « À l'État de mettre en place une identification électronique fiable » (cf. 21.3124, 21.3125, 21.3126, 21.3127, 21.3128 et 21.3129) qui ont été déposées par tous les groupes parlementaires qui ont été soumises suite au rejet de l'ancien projet de loi lors de la votation du 7 mars 2021. Selon les motionnaires, l'identité électronique étatique doit respecter les principes suivants: prendre en compte la protection de la vie privée dès la conception du produit (*privacy by design*), ne collecter que les données nécessaires et enregistrer celles-ci de manière décentralisée (par exemple auprès de l'utilisateur en ce qui concerne les données d'identification). La présente lettre reformule ces exigences en tant que buts spécifiques à atteindre dans le cadre de la protection des données personnelles.

La nLPD s'applique au traitement de données personnelles effectué dans le cadre de la mise œuvre du présent projet de loi. Afin d'éviter des répétitions et de faciliter la compréhension, les dispositions de l'avant-projet de loi ne renvoient pas aux articles pertinents de la nLPD (cf. ch. 6.8 protection des données).

Let. c

La présente lettre vise à garantir que la conception de l'e-ID et de l'infrastructure de confiance corresponde à l'état actuel de la technique.[17] Avec l'emploi de cette notion, le législateur vise un niveau élevé de sécurité et de protection des données grâce à des procédures avancées. A cet effet, il convient d'encourager l'examen régulier des mesures de sécurité mises en œuvre quant à leur efficacité par rapport aux objectifs de protection requis, leur actualité et leur degré d'innovation. Il en résulte également une comparaison des mesures de sécurité avec les produits de sécurité existants sur le marché.[18]

Let. d

Afin de faciliter l'obtention et l'utilisation de l'e-ID, l'avant-projet de loi établit des nouveaux standards ou harmonise les standards existants concernant l'émission, la vérification et la révocation de l'e-ID. Il vise également à assurer la sécurité de l'infrastructure et des processus d'émission et de vérification des autres moyens de preuve électroniques. Afin d'atteindre ces buts, il convient toutefois de ne pas limiter le progrès technique. Ainsi, l'avant-projet de loi ne règle le choix de la solution technique que lorsque cela est absolument nécessaire pour atteindre les objectifs législatifs. Il prévoit notamment une gestion décentralisée des données et exclut ainsi toute solution technique selon laquelle un fournisseur de services d'identification s'interpose entre le titulaire et le vérificateur d'un moyen de preuve électronique. Cela permet d'éviter de laisser une trace chez un tel fournisseur et de donner aux titulaires un plus grand contrôle sur leurs données.

15 Ibid; Biaggini, G., ibid, art. 81 N. 3
16 FF **2020** 7397
17 La notion de « état actuel de la technique » se distingue conceptuellement des autres états technologiques similaires tels que les « règles reconnues de la technique » et « état de la science et de la recherche ». En termes simples, le terme « état actuel de la technique » est plus innovant que le terme « règles reconnues de la technique » et plus obsolète que le terme « état de la science et de la recherche ». Cette distinction est la base essentielle pour déterminer le niveau de sécurité exigé. L'art. 7, al. 2 nLPD exige également la prise de mesures qui correspondent à « l'état de la technique », mais n'établit pas de critères pour déterminer ce qu'il faut entendre par « état de la technique ». Ce fait ne doit toutefois pas mener à la conclusion que ce qui n'est pas défini concrètement dans la loi ne peut pas être vérifié et par conséquent, ne peut pas être appliqué.
18 Ce qui est considéré aujourd'hui comme correspondant à « l'état de la technique » peut être considéré demain en raison du décalage dû à l'innovation, c'est-à-dire de l'obsolescence de la mesure de sécurité par rapport à des autres mesures de sécurité disponibles, comme une des « règles reconnues de la technique ».

Toutefois, la majorité des questions relatives au choix de la technologie ne sont pas réglées au niveau de la loi. Le progrès technique avançant à grand pas, il convient de s'assurer que le présent avant-projet de loi pourra être mis en œuvre dans le contexte technologique qui se présentera suite à son entrée en vigueur et qui n'est pas connu actuellement. Différents aspects à régler au niveau de l'ordonnance seront beaucoup plus équivoques sur le plan technologique, voire même plus spécifiques à la technologie. L'ordonnance devra garantir l'interopérabilité de tous les systèmes impliqués dans la communication. Pour ce faire, elle devra notamment définir très précisément les formats de données et les interfaces. Dans ce cadre, il conviendra de respecter le principe selon lequel seules les décisions technologiques absolument nécessaires doivent être prises. Ainsi, dans la mesure du possible, il convient de laisser aux acteurs impliqués le choix de la technologie qu'ils entendent utilisent pour formater, stocker et traiter les données de leur côté de l'interface.

Section 2 E-ID

Art. 2 Forme et contenu

Al. 1

La Confédération met en place une infrastructure de confiance (cf. Section 5) qui permettra à des acteurs publics et privés (cf. limitation de l'art. 18, al. 3) d'émettre divers moyens de preuve sous forme électronique qui pourront être utilisés en tant que justification de l'identité, d'un fait ou d'un événement (moyens de preuve électroniques). L'e-ID est un moyen de preuve électronique qui sera émise par fedpol au travers de l'infrastructure de confiance étatique.

Al. 2

Une e-ID contient les données d'identification personnelles de base suivantes: le nom officiel, les prénoms, la date de naissance, le genre, le lieu de naissance, la nationalité et la photographie enregistrée dans le système d'information relatif aux documents d'identité (ISA) ou le système d'information central sur la migration (SYMIC). Il s'agit de données disponibles dans les registres officiels de l'Etat auxquels fedpol à accès selon l'art. 11, al. 3. Suite à une demande de justification d'un vérificateur, le titulaire peut lui communiquer toutes ou certaines de ces données.

Al. 3

En sus des données d'identification personnelles de base, une e-ID contient des informations supplémentaires. Il s'agit des données suivantes: le numéro AVS, le numéro de l'e-ID, sa date d'émission, sa date de validité, le document d'identité qui a été utilisé lors de son émission, notamment son type, son numéro et sa date de validité et des indications relatives à la procédure d'émission (elles seront définies en détail par voie d'ordonnance).

Art. 3 Conditions personnelles

Remarque préliminaire

La formulation potestative de l'al. 1 garantit que les requérants n'ont aucune obligation d'obtenir ou d'utiliser une e-ID. Toutefois, une fois les conditions personnelles remplies, fedpol a l'obligation d'émettre une e-ID au requérant. Le requérant devient un titulaire lorsqu'il obtient l'e-ID.

Let. a

Pour demander l'émission d'une e-ID, il suffira au citoyen suisse d'avoir un document d'identité valable au sens de la LDI. Les personnes morales, agissant toujours par le biais de leur organe, autrement dit des personnes physiques, ne peuvent pas être titulaires d'une e-ID et sont identifiées au moyen d'un numéro d'identification unique des entreprises (IDE)[19].

Let. b

Tous les étrangers qui possèdent une autorisation valable au sens de la loi du 16 décembre 2005 sur les étrangers et l'intégration (LEI)[20] et l'ordonnance du 24 octobre 2007 relative à l'admission, au séjour et à l'exercice d'une activité lucrative (OASA)[21] pourront obtenir une e-ID. Il s'agit des permis suivants:

- Permis L : autorisation de courte durée (art. 32 LEI et art. 71, al. 1, OASA)
- Permis B : autorisation de séjour (art. 33 LEI et art. 71, al. 1, OASA)
- Permis C : autorisation d'établissement (art. 34 LEI et art. 71, al. 1, OASA)
- Permis Ci: autorisation de séjour avec activité lucrative (art 30, al. 1, let g et 98, al. 2 LEI et art. 45 et 71a, al. 1, let. e, OASA)
- Permis N : autorisation pour requérants d'asile (art. 42 LAsi et 71a, al. 1, let. b, OASA)
- Permis F : autorisation pour étrangers admis provisoirement (art. 41, al. 2, LEI et art. 71a, al. 1, let. c, OASA)
- Permis S : autorisation pour personnes à protéger (art. 74 LAsi et art. 71a, al. 1, d, OASA)
- Permis G : autorisation pour frontaliers (Art. 35 LEI et 71a, al. 1, let. a, OASA)

Il n'y a pas de différence fondamentale entre l'e-ID émise à l'intention des citoyens suisses et celle émise à l'intention des étrangers. En principe, l'e-ID peut être utilisée de la même manière par les citoyens suisses et par les étrangers. Toutefois,

19 Cf. www.bfs.admin.ch/bfs/fr/home/registres/registre-entreprises/numero-identification-entreprises.htm.
20 RS **142.20**
21 RS **142.201**

l'obtention d'une e-ID ne garantit pas au titulaire l'accès à tous les services qui y sont liés. Par exemple, il n'est pas certain qu'elle puisse lui permettre de bénéficier de tous les services offerts en ligne. En effet, certains prestataires pourront décider – pour des raisons de sécurité liées à la fiabilité de la vérification de l'identité des étrangers – de limiter l'accès à leurs services aux titulaires d'un certain type de permis de séjour. Le présent avant-projet de loi n'introduit pas de limitations d'accès aux services en ligne et laisse une marge de manœuvre en la matière aux prestataires de services concernés.

Pour certaines catégories de permis (p.ex. les permis N, F, S et Ci), il n'est pas certain d'emblée que l'identité ait pu être vérifiée de façon fiable. Nombreux sont les demandeurs d'asile qui ne sont pas en mesure de présenter un document d'identité au cours de la procédure d'asile et qui ne peuvent donc pas être identifiés de façon fiable. Le DFJP (SEM) reçoit de nombreuses demandes de changement ou de rectification des données d'identification personnelles pour les personnes admises à titre provisoire, bien souvent sans que ces demandes soient attestées par des documents adaptés. Comme chaque e-ID inclut des données concernant le document d'identité qui a servi à son émission, il semble justifié d'introduire la possibilité de reconnaître les e-ID qui ont été émises à l'intention des étrangers. Lorsque cela est justifié et prévu expressément par la loi, il est possible de limiter l'accès à certains services aux titulaires d'un permis étranger dont l'identité n'a pas pu être vérifiée de façon fiable.

Afin d'augmenter son efficacité et sa rapidité, la procédure d'obtention de l'e-ID se fonde sur la présentation d'une preuve d'identité suisse valide. Il a été également envisagé de procéder à une nouvelle vérification de l'identité du requérant. Cette possibilité a toutefois été abandonné pour des raisons de coûts, de convivialité et de rapidité. En effet, cette démarche aurait été plus coûteuse que l'obtention d'un document d'identité.

Art. 4 Émission

Remarque préliminaire

Le requérant pose une demande auprès de fedpol, qui lance la procédure d'émission lorsque les conditions personnelles visées à l'art. 3 sont remplies.

Al. 1

Il n'y a pas d'obligation d'obtenir une e-ID. Si quelqu'un veut en obtenir une, il devra la requérir auprès de fedpol. La demande doit émaner du futur titulaire de l'e-ID (requérant) ou de son représentant légal (voir al. 2, pour les mineurs et les personnes sous curatelle de portée générale). Le requérant ou le représentant légal pourra déposer une demande d'émission d'une e-ID directement au travers du système d'information de fedpol ou de son portefeuille électronique.

Al. 2

Selon cet alinéa, les mineurs de moins de 14 ans ainsi que les personnes sous curatelle de portée générale requièrent l'autorisation de leur représentant légal pour l'obtention de l'e-ID. La limite d'âge prévue pour les mineurs se fonde sur l'art. 8 de du règlement UE No. 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[22], selon lequel « (...) le traitement des données à caractère personnel relatives à un enfant est licite lorsque l'enfant est âgé d'au moins 16 ans » (al. 1). En outre, « [l]es États membres peuvent prévoir par la loi un âge inférieur pour ces finalités pour autant que cet âge inférieur ne soit pas en-dessous de 13 ans ». La Suisse n'a pas d'obligation juridique de respecter les exigences de l'art. 8. Par ailleurs, la teneur de cette article n'a pas été reprise dans le cadre de la reforme de loi sur la protection des données. Toutefois, la lex specialis en matière d'identification électronique peut restreindre l'accès des enfants et des personnes sous curatelle de portée générale. Ces personnes méritent une protection spécifique car elles sont moins conscientes des risques, des conséquences, des garanties et de leurs droits liés au traitement des données personnelles. Cette restriction d'âge pour l'obtention d'une e-ID est moins élevée que celle pour l'obtention des documents d'identité suisses (soit 18 ans; art. 5, al. 1, loi sur les documents d'identité). Comme les adolescents utilisent principalement l'internet pour accomplir leurs tâches quotidiennes, l'avant-projet de loi vise à leur permettre d'obtenir une e-ID à partir du moment qu'ils comprennent les conséquences du traitement des leurs données personnelles. Le but principal de cet alinéa est de protéger les personnes concernées mais également de ne pas restreindre indûment leurs activités dans le monde numérique.

Al. 3

fedpol s'assure que requérant remplit les conditions définies à l'art. 3. Si tel est le cas, il procède à la vérification de son identité au moyen des informations requises. Il compare les informations fournies par le requérant avec celles issues des registres fédéraux selon l'art. 11, al. 3 pour vérifier son identité. Lorsque l'identité du requérant a été vérifiée avec succès, fedpol lui communique une e-ID avec les données visées à l'art. 2, al. 2 et 3.

Al. 4

Le présent alinéa met en œuvre les exigences de l'art. 34, al. 2, let. a nLPD. Selon cet article, une base légale dans une loi au sens formel est requise pour permettre aux organes fédéraux de traiter des données sensibles. Selon l'art. 5, let c, ch 4 nLPD, « les données biométriques identifiant une personne physique de manière univoque » constituent des données sensibles. Par données biométriques on entend « les données personnelles résultant d'un traitement technique spécifique et relatives aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique qui permettent

22 Règlement UE No. 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, JO L-119 du 4.5.2016, p. 1-88.

ou confirment son identification unique. »[23]. Ainsi, le présent alinéa met en place une base légale au sens formel permettant au Conseil fédéral de prévoir par voie d'ordonnance l'utilisation de la photographie visée à l'art. 2, al. 2, let. g et les données biométriques prélevées pendant l'émission de l'e-ID. Cette démarche est nécessaire pour vérifier que l'image faciale enregistrée par le requérant lors du processus d'émission correspond bien à celle contenue dans les registres fédéraux ISA ou SYMIC.

Al. 5

Le Conseil fédéral précisera les modalités de la procédure d'émission dans une ordonnance, où il fixera notamment le déroulement de la procédure et les normes et les protocoles techniques applicables à la communication des données.

Art. 5 Révocation

L'avant-projet de loi prévoit la possibilité de révoquer une e-ID dans les cas visés aux let. a à e. Du point de vue technique le titulaire ne peut pas bloquer ou suspendre une e-ID en raison du caractère décentralisé du système d'émission de l'e-ID. Le titulaire ou le représentant légal d'un mineur de moins de quatorze ans ou d'une personne sous curatelle de portée générale peut demander la révocation de son e-ID ou de l'e-ID de la personne qu'il représente. En outre, fedpol révoque l'e-ID s'il existe un soupçon fondé d'utilisation abusive d'une e-ID. Avant de procéder à une révocation, fedpol vérifie les informations qui lui ont été soumises. fedpol révoque également l'e-ID s'il prend connaissance du décès de son titulaire, du retrait du document d'identité utilisé lors de l'émission de l'e-ID ou de la modification des données d'identification personnelles visées à l'art. 2, al. 2. En outre, l'e-ID est révoquée lorsque le titulaire en obtient une nouvelle. Une e-ID révoquée ne peut plus être réactivée: la personne intéressée peut poser une nouvelle demande d'émission au sens de l'art. 4, al. 1 auprès de fedpol.

Art. 6 Durée de validité

Pour des raisons de sécurité, l'e-ID a une durée de validité limitée dans le temps. Le Conseil fédéral règle les exigences relatives à cette durée dans une ordonnance. Dans ce cadre, il conviendra de clarifier si la durée de validité de l'e-ID doit correspondre à celle du document qui a servi lors de son émission. La durée de validité sera indiquée dans l'e-ID (art. 2, al. 3, let. d). Si ce document d'identité utilisé lors de l'émission de l'e-ID est retiré par les autorités, l'e-ID est révoquée par fedpol au moment où il prend connaissance du retrait (art. 5, let. d, ch. 1).

Suite à l'expiration de sa validité, l'e-ID reste disponible sur le support électronique du titulaire en tant que moyen de preuve électronique authentique mais échu.

Art. 7 Devoir de diligence

Al. 1

Les obligations des titulaires d'une e-ID établies dans l'avant-projet de loi correspondent à peu près aux devoirs de diligence qui doivent habituellement être respectés lors de l'utilisation d'une carte de crédit ou d'une carte bancaire. Il est par exemple nécessaire et raisonnablement exigible de ne pas révéler le code PIN éventuel et de ne pas le conserver au même endroit que le support de l'e-ID. Il est également raisonnablement exigible d'activer les fonctions de restriction d'accès à l'appareil mobile qui sert de support de l'e-ID, par exemple la reconnaissance des empreintes digitales ou le code PIN, ou d'installer un logiciel antivirus sur ce support.

Malgré toutes les précautions possibles, personne n'est totalement à l'abri d'un vol d'identité. Des sanctions pénales adéquates pour punir un tel comportement devraient être mises en place. La nLPD complète le code pénal par un art. 179^{decies}, une disposition punissant l'usurpation d'identité d'une peine privative de liberté d'un an au plus ou d'une peine pécuniaire. Afin d'éviter des redondances, l'avant-projet de loi ne contient pas de dispositions sanctionnant le même comportement.

Al. 2

Le titulaire est tenu d'informer fedpol sans délai de tout soupçon d'utilisation abusive de son e-ID. Il peut s'agir par exemple d'événements qui se produisent suite à la perte du support de l'e-ID ou des informations provenant de tiers concernant une utilisation peu usuelle de l'e-ID.

Art. 8 Points de contact cantonaux

La transformation numérique est en cours aussi bien au niveau fédéral, cantonal que communal. L'e-ID permet d'accéder à divers processus numérisés, qui facilitent l'exécution des transactions en ligne. Comme certaines tâches ou activités peuvent être effectuées depuis chez soi, la présence physique de la personne concernée n'est plus requise. Malgré cette tendance à la numérisation de la société, certaines parts de la population ne sont pas prêtes à affronter ce changement. Ayant besoin d'assistance, elles préfèrent se déplacer pour consulter une autorité dans le monde réel. Les cantons ont déjà mis en place différents offres et services destinés aux personnes souhaitant obtenir un soutien ou des informations générales. De ce fait, le présent article prévoit la désignation des services cantonaux chargés de donner de l'assistance aux personnes intéressées. Il appartiendra aux cantons de déterminer comment ils désigneront et organiseront ces services de soutien. Ces points de contact cantonaux fourniront une assistance générale en lien avec différents processus cyberadministratifs, qui sera complémentaire au support technique fourni par fedpol concernant l'émission, l'utilisation ou la révocation de l'e-ID.

La plupart des cas d'assistance liés à la numérisation risquent de se présenter au niveau cantonal. Ainsi, les cantons sont appelés à désigner des points de contacts à proximité des personnes qui pourraient en avoir besoin (y compris en lien

[23] Message concernant la loi fédérale sur la révision totale de la loi fédérale sur la protection des données et sur la modification d'autres lois fédérale, FF **2017**, 6565, 6640-6641.

avec l'e-ID). Certains cantons ont déjà mis en place des services similaires. Dans le canton du Jura, par exemple, un système de points de contact offre de l'assistance de proximité dans le cadre des services cyber-administratifs cantonaux. À l'échelle internationale, le Danemark a également opté pour une telle approche.

Au niveau fédéral, la Confédération fournira une assistance aux services cantonaux pour les aspects liés à l'infrastructure de confiance (le second niveau de support).

Art. 9 Obligation d'accepter l'identité électronique

Les autorités et les services accomplissant des tâches publiques doivent accepter l'e-ID étatique au sens du présent avant-projet de loi lorsqu'ils recourent à l'identification électronique. Les autorités des cantons et des communes sont incluses parmi les destinataires de cette norme. Cela est indiqué parce que l'e-ID est conçue en tant qu'un moyen d'identification électronique étatique pour prouver sa propre identité dans le monde virtuel; elle est donc comparable à la carte d'identité et au passeport dans le monde physique, qui sont également acceptés par toutes les autorités lors de chaque identification. Cette obligation ne s'applique qu'aux processus d'identification nécessitant la présence du titulaire et la présentation d'une pièce d'identité. Elle ne concerne pas les solutions de login cantonales et communales existantes.

L'e-ID étatique pourra être utilisée conjointement avec les moyens d'accès aux services cyber-administratifs existants. Cette disposition reflète l'importance des e-ID au sens de la présente loi et de leur accueil par la population, mises en évidence par la «Stratégie Suisse numérique»[24] et la «Stratégie suisse de cyberadministration 2020–2023»[25]. Il s'agit notamment de soutenir les investissements de la Confédération destinés à la mise en œuvre des e-ID et de contribuer à la diffusion de celles-ci dans la cyberadministration, ce qui profitera non seulement à la Confédération, aux cantons et aux communes, qui pourront ainsi faire des économies à moyen terme, mais aussi à la population suisse.

Les questions liées à l'utilisation de l'e-ID ainsi que les conséquences juridiques s'y rapportant ne sont pas réglées dans l'avant-projet de loi. Ces questions doivent être réglées de manière spécifique pour chaque secteur. L'avant-projet de loi tient notamment compte du dossier électronique du patient et des poursuites pour dettes et de la faillite. Lors de la consultation, d'autres cas de figure seront examinés et, le cas échéant, l'avant-projet de loi sera complété.

Art. 10 Présentation d'une e-ID

Le présent article vise à s'assurer que les titulaires ne seront pas obligés de présenter leur e-ID dans le cadre de leurs interactions dans le monde réel. Malgré les avantages offerts par l'e-ID, il s'agit de ne pas exclure la possibilité de présenter des documents d'identité (physiques) dans ces cas de figure. Ainsi, lorsqu'il est possible d'identifier une personne au moyen d'une document d'identité dans le cadre d'un processus requérant sa présence, la présentation de l'e-ID (ou des parties de celle-ci) ne peut être offerte qu'à titre optionnel.

Art. 11 Système d'information pour l'émission et la révocation des e-ID

Al. 1

fedpol exploitera un système d'information qui traitera les données personnelles visées à l'art. 2. Le système d'information permettra de recevoir les demandes des requérants et d'assurer l'exécution des tâches de fedpol dans le cadre de l'émission et de la révocation des e-ID.

Al. 2

Le système d'information contient les données supplémentaires visées à l'art. 2, al. 3 ainsi que les données liées à la révocation d'une e-ID. En outre, on y conserve également les données, dites secondaires, créés durant le processus de vérification de l'identité et d'émission de l'e-ID, qui sont requises à des fins d'analyse statistique, d'assistance et de prévention d'abus. Les données personnelles sont consultées directement dans les registres fédéraux et ne sont pas sauvegardées dans le système (cf. al. 3).

Al. 3

Le système d'information pourra consulter les registres de personnes suivants, gérés au niveau fédéral, dans le but d'émettre l'e-ID:

- le système d'information relatif aux documents d'identité (ISA);
- le système d'information central sur la migration (SYMIC);
- le registre informatisé de l'état civil (Infostar) visé à l'art. 39 du code civil (CC)[26] et à l'art. 6a de l'ordonnance du 28 avril 2004 sur l'état civil (OEC)[27];
- le registre central de la centrale de compensation de l'AVS (CdC-UPI) visé à l'art. 71 loi du 20 décembre 1946 sur l'assurance-vieillesse et survivants (LAVS)[28].

fedpol pourra ainsi exécuter les tâches requises pour l'émission des e-ID d'une manière automatisée. Sur cette base, fedpol peut vérifier l'identité du requérant et lui communiquer les données visées à l'art 2, al. 3 au travers d'un canal sécurisé. Les données consultées ne sont ni dupliquées ni sauvegardées dans le système d'information de fedpol.

24 Cf. www.uvek.admin.ch/uvek/fr/home/communication/suisse-numerique.html.
25 Cf. www.administration-numerique-suisse.ch/application/files/5216/3636/7679/E-Government-Strategie-Schweiz-2020-2023_F_def.pdf.
26 RS **210**
27 RS **211.112.2**
28 RS **831.10**

Al. 4

Le Conseil fédéral règle par voie d'ordonnance les délais de conservation des différents types de données. Les données visées aux al. 2 et 3 peuvent être conservées pendant 5 ans suivant l'expiration de l'e-ID. La conservation des données vise à permettre d'examiner des cas d'abus éventuels.

Section 3 Autres moyens de preuve électroniques

Art. 12 Emission

Al. 1

Les autorités et les personnes privées (cf. limitation de l'art. 18, al. 3), peuvent utiliser l'infrastructure de confiance de la Confédération visée à la section 5 pour émettre des moyens de preuve électroniques (autres que l'e-ID étatique émise uniquement par fedpol). Il s'agit d'une disposition potestative qui n'oblige pas les autorités et les personnes privées à s'en servir. En outre, cet alinéa ne limite pas les types de moyens de preuve électroniques qui peuvent être émis; il vise à ouvrir l'infrastructure de confiance à divers acteurs et à leur permettre d'émettre des justificatifs électroniques de tous genres.

Al. 2

Les moyens de preuve électroniques sont composés de données diverses. En sus du contenu de base retenu par l'émetteur, elles doivent contenir son identifiant et la date d'émission du moyen de preuve électronique.

Art. 13 Révocation

Le présent article reflète la pratique actuelle, selon laquelle les émetteurs révoquent eux-mêmes les moyens de preuve électroniques qu'ils ont émis. Des tiers, soit des autorités ou des personnes physiques, n'ont pas la compétence de révoquer des justificatifs électroniques émis par d'autres acteurs. En outre, le présent article reprend certaines exigences applicables à la révocation de l'e-ID. Il vise à mettre en place des exigences minimales communes afin de protéger les titulaires des moyens de preuve électroniques lorsque le contrat conclu avec l'émetteur, le droit cantonal ou le droit des obligations ne prévoit pas d'exigences similaires. Ainsi, il permet au titulaire et au représentant légal d'un mineur de moins de 14 ans ou d'une personne sous curatelle de portée générale de demander la révocation de son moyen de preuve électronique ou de celui de la personne qu'il représente. En outre, l'émetteur est tenu de révoquer un moyen de preuve électronique s'il existe un soupçon fondé d'utilisation abusive d'un moyen de preuve électronique. Avant de procéder à une révocation, l'émetteur vérifie les informations qui lui ont été soumises. Un moyen de preuve électronique révoqué ne peut plus être réactivé: la personne intéressée peut poser une nouvelle demande d'émission auprès d'un émetteur.

Section 4 Utilisation des moyens de preuve électroniques

Art 14 Forme et conservation des moyens de preuve électroniques

Le titulaire reçoit une preuve électronique sous forme d'un paquet de données. Ce paquet de données est stocké sur un support technique appartenant au titulaire et est entièrement sous son contrôle (les tiers n'y ont pas accès). L'avant-projet de loi ne contient pas d'exigences par rapport aux moyens techniques qui doivent être utilisés pour conserver un moyen de preuve électronique. Le choix du support technique appartient au titulaire du moyen de preuve électronique.

Art. 15 Transmissibilité des moyens de preuve électroniques

Al. 1

Le présent alinéa interdit la transmissibilité à un tiers d'une preuve électronique personnalisée (délivrée à une personne physique)[29]. Il reflète une pratique croissante des émetteurs, qui vise à éviter des cas d'utilisation abusive au travers de l'émission des moyens de preuve électroniques personnalisés. Une telle mesure de protection des utilisateurs est particulièrement importante dans le cadre d'une infrastructure de confiance mise à disposition par la Confédération.

Al. 2

Suite à un changement de support technique (smartphone, ordinateur, etc.), le titulaire peut normalement restaurer les applications qu'il avait installées sur un ancien support. La Confédération pourra offrir cette même possibilité aux titulaires de moyens de preuve électroniques au travers de la mise ne place du système de copies de sécurité visé à l'art. 21. Ainsi, les moyens de preuve électroniques que le titulaire aura téléchargés sur un ancien support technique pourront être restaurés avec peu d'effort sur un nouveau support. Le transfert des moyens preuve électroniques vers le système de copies de sécurité visé à l'art. 21 permettra d'offrir cette possibilité de restauration rapide aux titulaires. Le présent alinéa délègue au Conseil fédéral la compétence d'édicter les prescriptions techniques qui seront requises pour un tel transfert des moyens de preuve électroniques

29 Pour la présentation des moyens de preuve électroniques, voir l'art. 16.

Art. 16 Présentation des moyens de preuve électroniques

Al. 1

Le titulaire n'est pas obligé de présenter ses moyens de preuve électroniques dans leur intégralité. Il est libre de décider quelles parties ou informations découlant d'un moyen de preuve électronique il présentera au vérificateur pour atteindre le but de la vérification requise dans un cas concret. L'avant-projet de loi ne contient pas d'exigences par rapport aux types de données qui doivent être communiqués lors du contrôle des moyens de preuve électroniques. C'est au vérificateur de définir les données requises en l'occurrence. La marge de manœuvre du titulaire est ainsi limitée par les exigences que les vérificateurs posent dans le cadre du processus de vérification. Si le titulaire décide de ne pas transférer les éléments requis, il ne pourra pas faire valoir son moyen de preuve électronique. La loi sur la protection de données pose toutefois des limites à ce que les vérificateurs peuvent exiger d'un titulaire de preuve électronique; ils sont notamment tenus de respecter le principe de finalité, de proportionnalité et de la minimisation des données. Cela signifie que les vérificateurs ne peuvent traiter que les données personnelles adéquates, pertinentes et nécessaires au regard des finalités pour lesquelles elles sont traitées. S'agissant des principes généraux de la protection des données personnelles qui s'appliquent indépendamment de la présente loi, il n'est pas nécessaire de le mentionner de manière explicite dans l'avant-projet de loi.

Al. 2

Les systèmes visés à la section 5 ne permettent pas à l'émetteur d'avoir accès aux informations liées à la présentation et à la vérification d'un moyen de preuve électronique. Ils sont conçus de manière à ce qu'un tel accès ne soit pas possible au niveau technique.

Al. 3

Les systèmes visés à la section 5 sont conçus de manière à ce que l'exploitant n'ait pas connaissance du contenu des preuves électroniques présentées. Dans la mesure du possible, les systèmes doivent être conçus de manière à ce qu'aucune conclusion ne puisse être tirée sur l'utilisation des preuves électroniques et sur les autorités et les personnes privées impliquées.

Section 5 Infrastructure de confiance

Remarques préliminaires

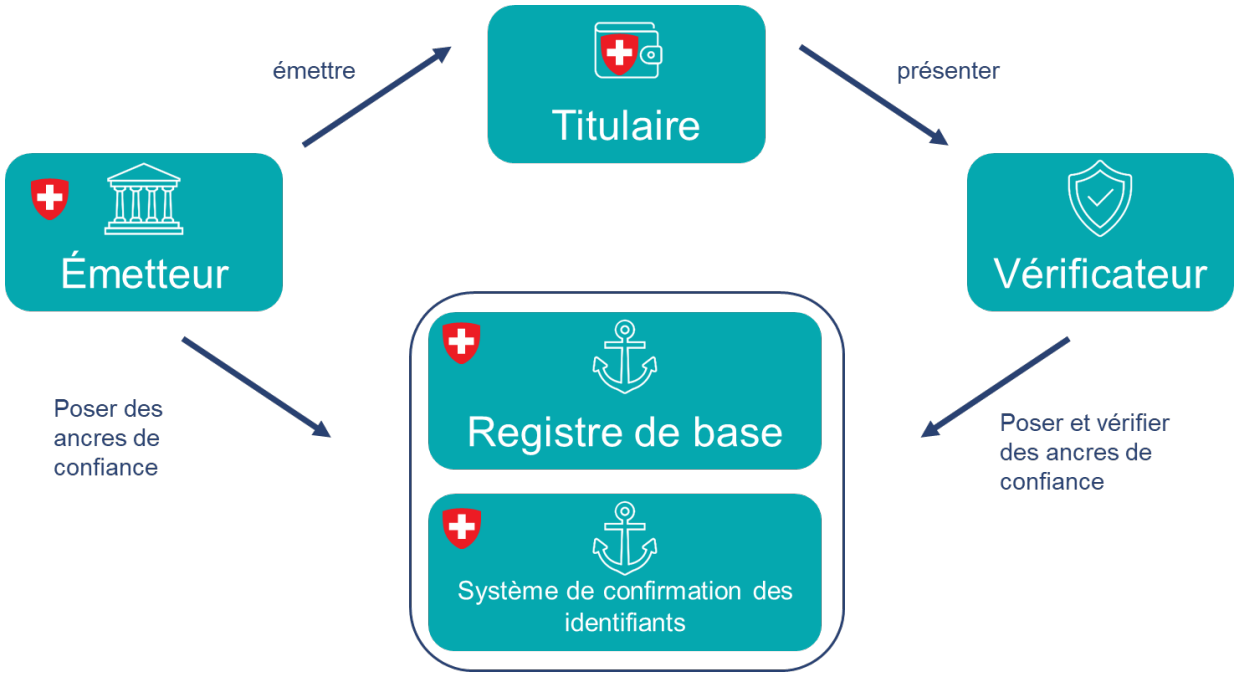
La Confédération a la compétence d'exploiter et de développer une infrastructure informatique permettant d'émettre, d'utiliser, de gérer, de valider et de révoquer des moyens de preuve électroniques. Il s'agit d'un ensemble de règlements, de processus, de concepts et d'éléments d'infrastructure qui garantissent la confiance dans les processus numériques et leur conformité et sont acceptés et utilisés par un large public. Dans ce cadre, la Confédération réalise et exploite l'infrastructure informatique dans l'intérêt du pays au sens de l'art. 81 Cst. La présente section s'écarte ainsi d'une interprétation stricte de l'art. 81 Cst, selon laquelle les travaux publics constituent des ouvrages matériels ou physiques, tel un bâtiment ou un tunnel. En raison du progrès technique et économique, il convient d'interpréter le concept de « travaux publics » d'une manière mieux adaptée aux développements récents[30], soit en tant qu'un ouvrage immatériel ou non-tangible, tel un système informatique ou un système de communication d'envergure comparable à l'infrastructure de confiance envisagée.

L'infrastructure de confiance vise à permettre l'émission et l'utilisation des e-ID et d'autres moyens de preuve électroniques. Une telle ouverture du système s'avère nécessaire au vu des développements techniques et économiques à l'échelle internationale et européenne.

Il n'est pas encore déterminé quels services de l'administration fédérale seront responsables de la mise en place et de l'exploitation des différents éléments de l'infrastructure de confiance. C'est pourquoi la section 5 parle encore de manière générale de « Confédération ». Sur la base des expériences faites avec les projets pilotes, cette question devra être clarifiée et fixée lors de l'élaboration du message.

30 Cf. Ch. 3.1.

L'infrastructure de confiance se compose des acteurs et des éléments suivants:



Art. 17 Registre de base

Al. 1

La Confédération met un registre de base à la disposition des autorités et des personnes privées intéressées. Il est un composant essentiel de l'infrastructure de confiance et constitue le premier volet de l'ancre de confiance du système : il permet à un vérificateur de contrôler que les moyens de preuves que lui présente le titulaire sont authentiques et intègres, tel que livrés par l'émetteur.

Le registre peut être mis en place sous forme distribuée (*distributed ledger technology, DLT*), par exemple à l'aide de la blockchain. Toutefois, le choix de la solution technique n'est pas réglé par l'avant-projet de loi, qui demeure, dans la mesure du possible, technologiquement neutre (cf. commentaire de l'art. 1, let. c).

Al. 2

Les informations enregistrées dans le registre de base comprennent: les identifiants de tous les émetteurs; les clés cryptographiques des émetteurs requises pour contrôler leurs identifiants et pour vérifier l'authenticité et l'intégrité des moyens de preuve électroniques; et les données relatives aux moyens de preuve électroniques révoqués. Ces données sont contenues dans le registre de base sous forme de chaînes de caractères alphanumériques et ne permettent pas de déduire l'identité des émetteurs et des vérificateurs. De plus, les adresses, les numéros de téléphone, les adresses email ou autres coordonnées des émetteurs et vérificateurs ainsi que les données personnelles des titulaires ne sont pas enregistrées dans le registre de base.

Al. 3

Les émetteurs inscrivent leurs données dans le registre de base, permettant ainsi à un vérificateur de contrôler l'authenticité et l'intégrité des moyens de preuve électroniques émis par l'émetteur concerné. Elles sont sécurisées par un algorithme cryptographique lors de l'inscription et sont considérées en tant qu'infalsifiables.

Les émetteurs et les vérificateurs voulant s'annoncer dans un système de confirmation des identifiants, doivent inscrire leurs informations dans le registre de base. Ce faisant, la vérification de l'identité des émetteurs ou des vérificateurs n'est pas nécessaire avant qu'ils ne puissent s'inscrire dans le registre de base. Cela impliquerait une procédure d'autorisation nécessitant des ressources importantes, ce qui conduirait inévitablement à un goulot d'étranglement coûteux et inutile. Certes, il existe un risque que des émetteurs ou des vérificateurs puissent délivrer des preuves électroniques en usurpant leur identité. Ce risque est toutefois atténué par la publication d'informations sur les cas de soupçons fondés d'utilisation abusive de l'infrastructure de confiance, conformément à l'art. 22, et exclu par le système de confirmation des identifiants prévu à l'art. 18. L'exclusion d'émetteurs ou de vérificateurs enregistrés n'est techniquement pas possible dans le registre de base, mais elle l'est dans le système de confirmation des identificateurs selon l'art. 18.

Al. 4

Le registre de base ne contient pas de données relatives aux moyens de preuve électroniques, telles les données personnelles ou matérielles ou les trace de l'émission des moyens de preuve électroniques. Les autorités et les personnes privées qui utilisent le registre de base n'ont pas accès aux données personnelles qui sont traitées dans le cadre de l'émission des moyens de preuve électroniques.

Art. 18 Système de confirmation des identifiants

Al. 1

La Confédération met en place un mécanisme étatique permettant de vérifier si un identifiant et une clé cryptographiques appartient à un émetteur inscrit dans le registre de base ou un vérificateur intéressé. Il constitue le deuxième volet de l'ancre de confiance du système : il permet aux titulaires et aux vérificateurs de savoir à qui ils ont effectivement à faire. La Confédération pourrait par exemple recourir à un répertoire de confiance ou à de certificats émis par une autorité compétente.

Un mécanisme de confirmation de l'identifiant vise à établir un lien entre le monde virtuel et le monde réel: il permet d'associer un identifiant technique inscrit dans le registre de base à une organisation, entité ou particulier existant dans le monde réel. Ce mécanisme est d'une grande importance pour les utilisateurs et les vérificateurs. Sachant qu'un vérificateur n'a pas forcément de relation directe avec un émetteur, le vérificateur peut recourir à ce mécanisme pour n'accepter des moyens de preuve électroniques que des émetteurs fiables. Par exemple, l'e-ID sera émise par fedpol, et l'identifiant technique de l'émetteur apparaîtra dans l'e-ID. Un vérificateur utilisera le mécanisme de confirmation de l'identifiant pour s'assurer que l'identifiant et les clés cryptographiques de l'émetteur de l'e-ID proviennent effectivement de fedpol.

La Confédération s'assure que le mécanisme de confirmation de l'identifiant est accessible à toute autorité et à toute personne privée intéressée. Cet accès leur permet de s'assurer que leur interlocuteur dans le monde virtuel est bien l'organisation, l'entité et la personne qu'il prétend être. Il permet de vérifier l'authenticité de la partie prenante à une transaction.

La mise en place du système de confirmation des identifiants des émetteurs et des vérificateurs sera effectuée en différentes étapes. Dès le début, la Confédération se voit déléguer la compétence de confirmer l'identité des autorités fédérales, cantonales et communales qui agissent en tant qu'émetteurs et vérificateurs. Elle charge une entité au sein de l'administration fédérale de gérer et d'entretenir le système de confirmation d'identité. Cette entité maintient une liste d'autorités agissant en tant qu'émetteurs et vérificateurs qu'elle publie sur son site et la met régulièrement à jour.

Al. 2

Le Conseil fédéral pourra éventuellement prévoir que la Confédération confirme l'identifiant et les clés cryptographiques des émetteurs et vérificateurs du secteur privé. Un tel besoin pourra se poser lorsque l'écosystème de l'e-ID se développera suffisamment et lorsque que la demande du secteur privé sera assez forte. Ainsi, le niveau de confiance dont bénéficie l'infrastructure de confiance dans le contexte de l'identification électronique pourra également être augmenté. Le Conseil fédéral pourra alors définir par voie d'ordonnance les exigences applicables à la confirmation de l'identifiant de ces organisations, entités et particuliers. Il s'agira également de prévoir les mesures techniques et organisationnelles qui seront à prendre dans ce cadre.

Il est possible que les acteurs du secteur privé décideront de mettre en place, à leur propre compte et séparément, un mécanisme de confirmation des identifiants non-étatique (privé); l'al. 2 ne limite pas leurs activités dans ce domaine.

Al. 3

Toute autorité et toute personne privée intéressée peut consulter les attributions des identifiants confirmées par le système dans le cadre du contrôle des moyens de preuve électroniques.

Art. 19 Application pour la conservation et la présentation des moyens de preuve électroniques

La Confédération établit une application pour la conservation et la présentation des moyens de preuve électroniques, dite portefeuille électronique étatique, aux personnes qui en font la demande. Il s'agit d'une application logicielle qui permet de demander et d'obtenir de manière sécurisée, stocker, sélectionner, combiner et partager des moyens de preuve électroniques d'une manière transparente et traçable pour l'utilisateur. L'e-ID comme tant d'autres moyens de preuve électroniques peut en faire partie. La mise en place du portefeuille électronique étatique suit autant que possible les standards qui sont présentement élaborés par l'Union européenne.

Le titulaire du portefeuille sauvegarde le moyen de preuve électronique dans un portefeuille électronique sur un support de son choix, tel un smartphone. Le vérificateur peut demander au titulaire de lui présenter des données via un canal de communication sécurisé. En réponse, le titulaire peut décider quelles données il transmet effectivement au vérificateur à partir de son portefeuille électronique.

La loi ne règle pas l'utilisation des portefeuilles électroniques émis par les acteurs privés. En sus du portefeuille électronique étatique, les utilisateurs peuvent se servir d'autres applications pour la conservation et la présentation de leurs moyens de preuve électroniques. La Confédération peut soumettre les prestataires offrant des portefeuilles électroniques à un processus d'évaluation et de certification selon l'art. 13 nLPD. Il n'est dont plus nécessaire de régler la possibilité de certification dans l'avant-projet de loi.

Art. 20 Système concernant la vérification des moyens de preuve électroniques

La présente disposition potestative permet au Conseil fédéral de mettre en place d'une application permettant de vérifier la validité des moyens de preuve électroniques. Il s'agit d'une mesure de sécurité supplémentaire qui pourra être prise en cas de besoin. Elle pourra notamment servir à augmenter la confiance dont bénéficie l'infrastructure de confiance au sein de la population.

Art. 21 Système des copies de sécurité

Al. 1

Suite à une perte ou à l'achat d'un nouveau smartphone, il est devenu habituel pour les utilisateurs de restaurer les applications installées à partir d'une sauvegarde. Ainsi, il est possible de récupérer rapidement les fonctionnalités de l'ancien système suite à un changement de smartphone. La même possibilité pourra être offerte aux titulaires de moyens de preuves électronique. Le présent alinéa délègue la compétence au Conseil fédéral de prévoir la mise en place d'un système informatique dans lequel les titulaires pourront sauvegarder des copies de leurs moyens de preuve électroniques. Suite à un changement de support technique (smartphone, ordinateur, etc.), ils pourront récupérer rapidement les moyens de preuve électroniques sauvegardés. Une telle sauvegarde des moyens de preuve électroniques pourra être prévue sur une nuage (cloud) ou localement sur le support technique du titulaire.

L'utilisation du système de copies de sécurité sera volontaire. Chaque titulaire sera libre de se prévaloir de l'option de sauvegarde de ses moyens de preuve électroniques.

Al. 2

Seuls les titulaires auront accès aux copies de sécurité protégées. Le système ne permet pas aux tiers d'y accéder.

Al. 3

Les copies de sécurité pourront être détruites à la demande de leur titulaire ou d'un représentant légal d'un mineur de moins de 14 ans ou d'une personne sous curatelle générale.

Art. 22 Utilisation abusive de l'infrastructure de confiance

En mettant à disposition une infrastructure de confiance, la Confédération s'engage également à mettre en place les mesures de sécurité requises afin de minimiser le risque d'utilisation abusive. L'exclusion des émetteurs du registre de base n'étant pas techniquement possible, l'avant-projet prévoit cette mesure afin de combattre les abus éventuels. Le présent article charge la Confédération de l'exploitation d'une plateforme servant à exposer les mauvaises pratiques et à avertir les autorités et la population en général des risques potentiels. Il ne faut toutefois assumer que les titulaires qui n'ont peut-être pas pris connaissance des informations ainsi publiées violent automatiquement leur devoir de diligence au sens de l'article 7, al. 1. En outre, la plateforme ne doit mentionner que les cas pour lesquels il existe un soupçon suffisamment fondé d'abus de l'infrastructure de confiance. Cette mesure doit être perçue en tant qu'une mesure complémentaire au système de confirmation des identifiants visant à protéger les utilisateurs et à assurer la transparence du fonctionnement de l'infrastructure de confiance.

L'avant-projet ne définit pas le terme « abus » afin de ne pas limiter indûment ou de ne pas exclure des cas d'abus éventuels. En outre, il s'agit de ne pas semer la confusion par rapport aux cas d'abus qui sont déjà réglés par la loi, comme par exemple l'usurpation de l'identité (art. 179^{decies} CP, introduit par la nLPD). L'abus visé par le présent article inclut les cas d'utilisation de l'infrastructure de confiance qui ne sont pas conformes aux but et exigences prévues par l'avant-projet.

Art. 23 Code source de l'infrastructure de confiance

La Confédération publie sur internet le code source des composants de l'infrastructure de confiance visée à la section 5. Les personnes intéressées pourront en prendre connaissance. Le développement du code et autres droits s'y rapportant ne sont pas réglés par le présent article; ils relèvent de l'art. 9 du projet de loi fédérale sur l'utilisation de moyens électroniques pour l'exécution des tâches des autorités (LMETA)[31].

Art. 24 Exploitation de l'infrastructure de confiance

L'exploitation des éléments de l'infrastructure de confiance est assurée par un prestataire de services aux sein de l'administration fédérale. Cet article permet d'assurer les exigences des six motions de même teneur intitulées « À l'État de mettre en place une identification électronique fiable » (cf. 21.3124, 21.3125, 21.3126, 21.3127, 21.3128 et 21.3129) qui demandent que le fonctionnement du système devra être assumé par des services publics spécialisés. Par ailleurs, cela permet également de garantir que la Confédération ne puisse pas exploiter l'ensemble de l'infrastructure de confiance en dehors de l'administration fédérale.

Art. 25 Progrès technique

Al. 1

Le progrès technique avance à grand pas et la technique continuera d'évoluer suite à l'entrée en vigueur du présent avant-projet de loi. Afin de s'assurer que celui-ci puisse être mis en œuvre, le présent article délègue la compétence au Conseil fédéral d'émettre par voie d'ordonnance des dispositions complémentaires permettant d'adapter l'infrastructure de confiance au progrès technique et de s'assurer qu'elle continue d'atteindre les objectifs définis par la présente loi.

Al. 2

Pour divers motifs, les dispositions complémentaires peuvent nécessiter la mise ne place d'une base légale formelle. Par exemple, selon l'art. 34, al. 2, let. a nLPD, il ne suffit pas de prévoir le traitement de données sensibles dans une ordonnance; une base légale dans une loi au sens formel est requise. Dans ce cas, l'ordonnance du Conseil fédéral devient caduque: si, dans un délai de deux ans après son entrée en vigueur, le Conseil fédéral n'a pas soumis à l'Assemblée

31 FF **2022** 805

fédérale un projet établissant la base légale de son contenu; si le projet est rejeté par l'Assemblée fédérale; ou si la base légale prévue entre en vigueur.

Section 6 Émoluments

Art. 26

Al. 1

Des émoluments seront perçus des émetteurs et des vérificateurs pour l'inscription de données (l'identifiant, le matériel cryptographique et les révocations des moyens de preuve électroniques) dans le registre de base et dans le système de confirmation des identifiants

Le montant des émoluments n'étant pas prévu dans la loi, il sera défini par voie d'ordonnance. Dans ce cadre, le législateur s'orientera vers les montants qui ont déjà été fixés dans la pratique.[32]

Al. 2

Si le Conseil fédéral décide de mettre en place le système des copies de sécurité visé à l'art. 21, il pourra prévoir par voie d'ordonnance des émoluments pour son utilisation.

Al. 3

Le Conseil fédéral règlera par voie d'ordonnance la perception des émoluments conformément à l'art. 46*a* de la loi du 21 mars 1997 sur l'organisation du gouvernement et de l'administration (LOGA)[33].

Al. 4

Les autres services fournis par la Confédération selon la présente loi sont gratuits. Ainsi, aucun émolument n'est perçu pour l'émission de l'e-ID ainsi que pour son utilisation et sa vérification. De plus, l'utilisation du portefeuille électronique émis par la Confédération, la lecture du registre de base et l'utilisation du mécanisme de confirmation de l'identifiant sont également non payantes.

En renonçant partiellement à la perception d'émoluments, l'utilisation et la diffusion de l'e-ID doivent être encouragées. La Confédération a tout intérêt à ce que l'utilisation de l'e-ID soit la plus répandue possible afin de faciliter les échanges avec les autorités et les personnes privées.

Section 7 Conventions internationales

Art. 27

Compte tenu de l'étroitesse des rapports commerciaux et sociaux qu'elle entretient avec la plupart des pays membres de l'UE, la Suisse a tout intérêt à se donner la possibilité d'être tôt ou tard intégrée dans le système européen pour l'interopérabilité des systèmes d'identification électronique avec le système européen et, le cas échéant, avec d'autres systèmes étrangers. Pour ce faire, un accord international sera requis. Le présent article délègue au Conseil fédéral la compétence pour conclure des accords internationaux destinées à faciliter l'utilisation et la reconnaissance sur le plan international de l'e-ID et il peut adopter les prescriptions d'exécution nécessaires. Un tel accord permettrait d'assurer à l'avenir la reconnaissance mutuelle du système d'identification suisse et de ceux notifiés selon le règlement eIDAS ou mis en place par certains membres de l'UE ou des États tiers.

Section 8 Dispositions finales

Art. 28 Dispositions d'exécution

Les dispositions d'exécution de la présente loi règlent la mise en œuvre des aspects techniques et organisationnels liés à la communication des moyens de preuve électroniques ainsi que le fonctionnement des composants de l'infrastructure de confiance. Il s'agira notamment de régler le format des moyens de preuve électroniques; les normes et protocoles applicables aux processus de communication des données lors de l'émission et de la présentation des moyens de preuve électroniques; les éléments et le fonctionnement du registre de base, du système de confirmation des identifiants, de l'application pour la conservation et la présentation des moyens de preuve électroniques et du système des copies de sécurité; les preuves à fournir pour l'inscription dans le système de confirmation des identifiants; les interfaces ainsi que les éléments et le fonctionnement du système d'information pour l'émission et la révocation des e-ID; et les rôles et les responsabilités des acteurs impliqués dans la mise à disposition et l'utilisation de l'infrastructure de confiance. Enfin, le Conseil fédéral se voit également déléguer la compétence de régler par voie d'ordonnance les mesures techniques et organisationnelles relatives à la sécurité et la protection des données, dans le cadre de l'exploitation et de l'utilisation de l'infrastructure de confiance.

32 Voir par exemple les indications fournies par la fondation Sovrin: https://sovrin.org/issue-credentials/
33 RS **172.010**

Ces dispositions d'exécution visent notamment à établir des nouveaux standards et à harmoniser les standards internationaux et européens existant en la matière afin de faciliter la mise en œuvre de la présente loi. Pour des raisons de clarté et de transparence, elles ont été réunies dans une seule disposition.

Art. 29 Modification d'autres actes

L'avant-projet propose la modification d'autres actes. Ces adaptations visent principalement à permettre à fedpol d'accéder aux systèmes d'information ISA, Infostar, et SYMIC. Elles règlent également, à titre indicatif, l'utilisation de l'e-ID dans certains secteurs, tels le dossier électronique du patient et le domaine de la faillite et des poursuites. Lors de la consultation, il s'agira d'examiner si d'autres lois fédérales devront être adaptées (ou si ces modifications pourront être effectuées par voie d'ordonnance).

Art. 30 Référendum et entrée en vigueur

Comme toute loi fédérale, l'avant-projet de loi est sujet au référendum et le Conseil fédéral est chargé de fixer la date de son entrée en vigueur.

Modifications d'autres actes

Remarque préliminaire

On estime à ce stade que les conditions d'identification et d'authentification pour les applications de la cyberadministration doivent, dans la mesure où elles sont nécessaires, être réglées par voie d'ordonnance ou de directive. Plusieurs ordonnances et directives devront être modifiées en vue de la mise en œuvre de la loi sur l'e-ID. Cela n'interviendra toutefois qu'au moment de l'adoption des dispositions d'exécution de la loi sur l'e-ID, raison pour laquelle seules les modifications d'autres lois fédérales sont expliquées dans la présente section.

1. Loi fédérale du 20 juin 2003 sur le système d'information commun aux domaines des étrangers et de l'asile (LDEA)[34]

Art. 9, al. 1, let. c, et 2, let. c, ch. 3 (nouveau)

L'art. 9, al. 1, énumère les autorités auxquelles le SEM peut donner accès en ligne aux données relevant du domaine des étrangers qu'il a traité ou fait traiter dans le système d'information régi par la LDEA. La let. c précise les buts pour lesquels un tel accès pourrait être donné aux autorités fédérales compétentes dans les domaines de la police. Il s'agit d'ajouter à cette liste un nouveau but, notamment l'accomplissement des tâches qui leur incombent en vertu du présent avant-projet de loi.

L'art. 9, al. 2, énumère les autorités auxquelles le SEM peut donner accès en ligne aux données relevant du domaine de l'asile qu'il a traité ou fait traiter dans le système d'information régi par la LDEA. La let. c énumère les buts dans lesquels un tel accès pourrait être donné aux autorités fédérales compétentes dans le domaine de la police. Le projet ajoute un nouveau but à cette liste, notamment l'accomplissement de leurs tâches visées par la loi sur l'e-ID.

2. Loi du 22 juin 2001 sur les documents d'identité (LDI)[35]

Art. 11, al. 2

L'art. 11, al. 2 énumère les finalités du traitement des données effectué dans cadre de l'exploitation de l'ISA par fedpol. La présente loi insère des chiffres dans l'énumération des finalités. En outre, il s'agit d'ajouter une nouvelle finalité du traitement, soit l'accomplissement des tâches visées par la loi sur l'e-ID.

3. Code civil[36]

Art. 43a, al. 4, ch. 9

L'art. 43*a* CC règle l'accès en ligne aux registres informatisés visant à gérer l'état civil. fedpol est ajouté à la liste des services qui ont accès à Infostar.

4. Loi du 11 avril 1889 sur la poursuite pour dettes et la faillite (LP)[37]

Comme indiqué dans les explications relatives aux art. 9 et 28, des questions telles que l'obligation de reconnaissance ou les conséquences juridiques de l'utilisation d'une identité électronique ne peuvent pas être réglées de manière générale dans la loi sur l'identité électronique, mais doivent être incluses à titre indicatif dans certains domaines juridiques. Dans le

34 RS **142.51**
35 RS **143.1**
36 RS **210**
37 RS **210**

cadre de la procédure de consultation, il conviendra d'examiner si des exigences similaires seront requises dans d'autres domaines.

Art. 8a, al. 2bis

Il existe différentes possibilités pour déposer une demande d'informations tirées du registre des poursuites : Se présenter au guichet de l'office des poursuites, déposer une demande écrite par courrier ou par voie électronique via l'une des différentes solutions de portail proposées par la Confédération, les cantons ou le secteur privé. Si la demande concerne un tiers, un intérêt doit être rendu vraisemblable conformément à l'art. 8a, al. 1, LP. Pour les extraits personnels, une preuve d'identification est requise ; celle-ci peut généralement être apportée par l'envoi d'une copie d'une carte d'identité ou d'un passeport. Dans le cas des solutions de portail, le processus de commande peut être simplifié pour toutes les personnes concernées si le requérant peut être identifié au moyen d'une e-ID. En outre, la qualité de l'identification - par rapport à une copie plus ou moins lisible (et facilement falsifiable) d'une carte d'identité ou d'un passeport - est nettement améliorée.

Art. 33a, al. 2bis

Conformément à l'art. 33a, al. 1, LP, les requêtes peuvent être déposées par voie électronique auprès des offices des poursuites et des faillites et des autorités de surveillance. Celles-ci doivent être munies d'une signature électronique qualifiée (art. 33a al. 2 LP), ce qui permet d'attribuer clairement la requête à une personne physique. Comme cette attribution univoque peut également être garantie par la présentation d'une carte d'identité électronique, il convient de renoncer à l'apposition d'une signature électronique qualifiée dans les solutions de portail de la Confédération ou d'un canton. Cela permet de simplifier le processus de saisie pour toutes les personnes concernées.

5. Loi du 19 juin 2015 sur le dossier électronique du patient (LDEP)[38]

Art. 7

Le présent avant-projet de loi remplace l'expression « identité électronique » mentionnée à l'art. 7 LDEP par « moyen d'identification ». Le « moyen d'identification » correspond mieux au sens du concept qui est réglé à cet article. En outre, il s'agit d'éviter toute confusion avec le présent avant-projet de loi, qui établit le cadre légal de l'identité électronique étatique. Cette dernière est une preuve d'identité d'une personne sous forme électronique et non un moyen d'identification qui permet de s'authentifier et d'accéder à un service ou une application. Pour des raisons de clarté, il convient de maintenir une distinction terminologique entre les deux lois et de modifier la LDEP.

Art. 11 let. c

Selon le système actuel de la LDEP, les moyens d'identification électroniques pour l'accès au dossier électronique du patient sont émis par des acteurs privés, qui doivent être certifiés par un organisme reconnu. À long terme, ces moyens d'identification seront également émis par la Confédération. Ainsi, la volonté politique du souverain exprimée lors de la votation populaire du 7 mars 2021, qui ne voulait pas que cette tâche soit confiée au secteur privé, sera également respectée dans le domaine de la LDEP.

Si la Confédération assume cette tâche, elle devra remplir les exigences prévues par la législation sur le dossier électronique du patient, mais une certification de l'organe fédéral compétent n'est pas requise à cette fin. Comme des moyens d'identification privés continueront d'être utilisés pendant une certaine période transitoire pour accéder au dossier électronique du patient, l'art. 11, let. c, stipule désormais que les éditeurs privés de moyens d'identification doivent continuer à être certifiés.

6. Loi du 18 mars 2016 sur la signature électronique (SCSE)[39]

Art. 9, al. 4bis

Toute personne qui demande la délivrance d'une signature électronique doit se présenter en personne. Elle n'est pas soumise à cette obligation si elle peut prouver son identité avec un moyen d'identification électronique au sens de la présente loi. Le Conseil fédéral peut prévoir par voie d'ordonnance que la présence de la personne concernée n'est pas nécessaire lorsque son identité peut être prouvée par d'autre moyens avec le niveau de fiabilité requis.

7. Loi fédérale du ... sur l'utilisation de moyens électroniques pour l'exécution des tâches des autorités (LMETA)[40]

Le présent avant-projet de loi établit le cadre légal applicable à l'identité électronique étatique. L'identité électronique permet au titulaire de s'identifier mais pas de s'authentifier pour accéder à un service en ligne ou à une application. Pour cette raison la présente loi modifie la future LMETA pour inclure un système d'authentification en tant que « moyens informatique » au sens de l'art. 11, al. 1 à 3 LMETA. Ce système d'authentification se fonde sur l'e-ID et peut donner accès à un service ou à une application.

38 RS **816.1**
39 RS **943.03**
40 FF **2022** 805

Ce système d'authentification des personnes physiques est également à la disposition, en tant que moyen TIC, des cantons et des communes. En outre, il peut être utilisé par des organisations et des personnes de droit public ou privé, dans la mesure où elles sont chargées de l'exécution du droit fédéral.

Les délibérations parlementaires sur la LMETA sont en cours. La loi n'a pas encore été adoptée par le Parlement, raison pour laquelle la modification prévue devra être réévaluée à l'issue des débats parlementaires...

5 Conséquences

5.1 Conséquences sur les finances et l'état du personnel pour la Confédération

Durant la phase initiale, le projet e-ID engendre des coûts pour les travaux législatifs ainsi que pour d'autres domaines, notamment la communication et l'accompagnement de projets connexes. Si la demande de financement du DFJP est acceptée, ces coûts pourront être défrayés par les fonds destinés à la réalisation de l'ambition 3 « Une identification numérique reconnue pour toutes les autorités est établie » de l'agenda de l'ANS. Pour 2022, les moyens demandés (CHF 750'000) ont été approuvés par les organes de l'organisation ANS. De plus, CHF 1'000'000 pour 2023 a été réservé à cet effet dans la planification préparatoire de l'organisation ANS.

Une estimation initiale des coûts liés au projet et à l'exploitation a été réalisée sur la base de l'expérience acquise dans le cadre de l'émission du certificat COVID. En outre, les essais pilotes prévus permettront de définir ces coûts plus précisément lors de l'élaboration du message.

Selon cette estimation, les coûts du projet se situent entre CHF 25 et 30 millions. Ils comprennent le développement et la mise en service de l'infrastructure de confiance. Ceci inclut le développement du système informatique ainsi que l'adaptation de l'infrastructure du service de l'identité de fedpol. Le projet durera entre 24 et 36 mois à compter de son lancement jusqu'à la mise en service (go live) de l'infrastructure de confiance.

Les coûts d'exploitation du projet sont évalués entre CHF 10 et 15 millions. En sus, il s'agira d'évaluer le dimensionnement du support qui devra être assuré au niveau de l'infrastructure de confiance ainsi qu'au niveau de l'émission de l'e-ID. La forme et le dimensionnement de ce support ne pourront être définis qu'après le retour d'expérience des essais pilotes et une évaluation des synergies potentielles entre les offices pour les systèmes existants et à venir.

Pour financer les investissements, des contributions financières sont demandées à l'ANS, car l'identification électronique inter-administrations fait partie des objectifs de l'agenda ANS. L'exploitation et le développement doivent être financés autant que possible par des émoluments.

5.2 Conséquences pour les cantons et les communes

Les cantons et les communes sont obligés d'accepter l'e-ID étatique lorsqu'ils recourent à l'identification électronique. Cela est indiqué parce que l'e-ID est conçue en tant que moyen d'identification électronique étatique pour prouver sa propre identité dans le monde virtuel; elle est donc comparable à la carte d'identité et au passeport dans le monde physique, qui sont également acceptés par toutes les autorités lors de chaque identification.

Les cantons et les communes utilisent divers systèmes de cyberadministration. Les processus d'identification et d'authentification permettant d'accéder à ces systèmes pourraient être considérablement simplifiés par la mise en place des e-ID et du recours à l'infrastructure de confiance. L'identification simple et sûre favorise l'utilisation des services de cyberadministration proposés par les villes et les communes.

En outre, l'infrastructure de confiance permettra aux cantons, communes et villes d'accomplir certaines tâches plus efficacement, par exemple d'émettre des permis de pêche électronique, des cartes de stationnement électroniques ou des attestations de domicile électroniques. Les émetteurs n'auront plus à s'occuper de l'application logicielle de l'utilisateur (portefeuille électronique) ni des mesures de sécurité, mais uniquement de leurs propres processus et systèmes de gestion. Dans cette optique, l'infrastructure de confiance permettra de progresser en matière de numérisation des activités publiques de tous les niveaux.

Il est difficile de chiffrer le coût de l'adaptation éventuelle des systèmes offerts par les cantons, les villes et les communes pour permettre l'identification par e-ID. Ces coûts devraient être couverts par les économies que les communes, les villes et les cantons feront à moyen terme grâce à la mise en place de processus numériques. En outre, l'utilisation de l'infrastructure de confiance de la Confédération permettra aux cantons d'éviter des coûts si, par exemple, ils ne doivent pas investir dans leur propre infrastructure et peuvent l'exploiter pour l'introduction d'un permis de conduire électronique. La loi prévoit qu'eux et les autres collectivités territoriales – comme les utilisateurs privés – paieront des frais pour l'inscription dans le registre de base et la confirmation de l'affiliation. Elles participeront ainsi au financement de l'exploitation de l'infrastructure de confiance de l'e-ID. Les coûts qui y sont liés sont toutefois bien inférieurs à ceux d'une infrastructure propre.

La transformation numérique est en cours aussi bien au niveau fédéral, cantonal que communal. Malgré cette tendance à la numérisation de la société, certaines parts de la population ne sont pas prêtes à affronter ce changement. Ayant besoin d'assistance, elles préfèrent se déplacer pour consulter une autorité dans le monde réel. Les cantons ont déjà mis en place différents offres et services destinés aux personnes souhaitant obtenir un soutien ou des informations générales. Ces points de contact existants pourront et devront également être utilisés pour offrir une assistance en rapport avec l'E-ID. Il appartiendra aux cantons de déterminer comment ils désigneront et organiseront ces services de soutien. Etant donné

qu'ils sont nécessaires en tant que soutien général et pas seulement pour l'e-ID, les conséquences peuvent être considérées comme faibles.

5.3 Conséquences économiques

Le Conseil fédéral a pour objectif d'apporter les contributions nécessaires à la numérisation de la société suisse. Dans ce but, il a pris de nombreuses mesures visant principalement à adapter le cadre légal ou à mettre en place les infrastructures requises.

L'introduction de l'identification électronique et de l'infrastructure de confiance sont des éléments clés pour la mise en place d'un vaste écosystème de moyens de preuve électroniques qui garantit la fiabilité et la sécurité des transactions électroniques. Les transactions complexes avec l'État ou entre des partenaires privés peuvent être effectuées électroniquement et donc de manière plus efficace.

5.4 Conséquences sociales

La numérisation de la société avance à grands pas. Un nombre grandissant de transactions peuvent désormais être effectuées en ligne; l'obligation de se présenter en personne devient de moins en moins pertinente. On s'attend de plus en plus à ce qu'il soit possible d'accomplir diverses tâches par voie électronique, et de préférence, sur un smartphone. Bien que les moyens de communications pour le faire ne manquent pas, il n'est pas encore possible de créer, de gérer et de de présenter des moyens de preuve électroniques qui soient suffisamment fonctionnels et acceptés par la plupart des prestataires. L'infrastructure de confiance de la Confédération vise à pallier à cette lacune; elle en met en place un écosystème qui permet d'émettre, d'utiliser et de présenter de manière sécurisé divers moyens de preuve électroniques. Il s'agit d'un ensemble de standards, de processus, de concepts et d'éléments d'infrastructure qui garantissent la confiance dans les processus numériques et leur conformité et sont acceptés et utilisés par un large public. Les transactions électroniques dans les secteur public et privé pourront être accomplies de manière plus efficace et plus sûre tout en respectant les exigences de la nLPD. Une telle infrastructure permet d'augmenter l'interconnectivité entre les divers acteurs et le niveau de confiance dont bénéficient les transactions électroniques.

En ce qui concerne l'e-ID, un de ses principaux avantages est la possibilité de présenter ses données à un interlocuteur sur internet. Le titulaire obtient non seulement plus de contrôle sur ses données, mais également plus de responsabilité, notamment en ce qui concerne le devoir de diligence, dans le cadre des transactions électroniques. L'étendue de cette responsabilité ainsi que ses conséquences seront définies plus précisément par voie d'ordonnance. En outre, la possession de l'e-ID requiert un certain niveau de connaissances par rapport au fonctionnement de son système. Le débat public concernant l'avant-projet de loi permettra déjà de développer une certaine sensibilisation en matière digitale au sein de la population suisse.

6 Aspects juridiques

6.1 Constitutionalité

La compétence de régler les e-ID et l'infrastructure de confiance découle des art. 38, al. 1, 81, 95, al. 1, et 121, al. 1 de la Constitution.

S'agissant de l'identité électronique étatique, l'avant-projet de loi repose sur l'art. 38, al. 1 et l'art. 121, al. 1 Cst. L'art. 38 al. 1 donne la compétence à la Confédération de régler l'acquisition et la perte de la nationalité et des droits de cité par filiation, par mariage ou par adoption. En outre, l'art. 121 al. 1 Cst confère la compétence à la Confédération de légiférer en matière d'entrée en Suisse, de sortie, de séjour et d'établissement des étrangers et d'octroi de l'asile. Bien que ces deux articles ne règlent pas expressément les documents d'identité, la Confédération doit avoir la compétence de régler les documents d'identité requis, même si ceux-ci ne servent pas exclusivement à prouver de nationalité des citoyens suisses et le statut de séjour des habitants étrangers. L'identité électronique (e-ID) étatique servant à remplacer ces documents dans certains secteurs d'activité, il est justifié de fonder le futur projet de loi sur ces bases constitutionnelles pour ce qui concerne les preuves officielles de l'identité, de la nationalité et du statut de séjour des étrangers.

La compétence de mettre en place une infrastructure de confiance est réglée à l'art. 81 Cst. Celui-ci permet à la Confédération de réaliser, dans l'intérêt du pays ou d'une grande partie de celui-ci, des travaux publics, d'exploiter elle-même des ouvrages publics ou d'encourager leur réalisation. Un « ouvrage » ou des « travaux publics » au sens de cette disposition sont traditionnellement de nature physique, au sens d'une construction, comme par exemple un tunnel. Toutefois, suivant l'interprétation évolutive et téléologique de Lendi[41] et de Biaggini[42], un « ouvrage » ou des « travaux publics » pourraient également être immatériels ou non-tangibles, tel un système informatique ou un système de communication d'envergure comparable à l'infrastructure de confiance envisagée. Il serait ainsi possible de fonder sur l'art. 81 un avant-projet de loi qui vise à mettre en place une infrastructure de confiance permettant d'émettre et de valider divers moyens de preuve électroniques. Dans ce cadre, il convient de rappeler que l'art. 81 Cst ne confère pas à la Confédération de compétence

41 DFJP, Bundesamt für Justiz, Rechtsgrundlagen für die IKT-Zusammenarbeit zwischen dem Bund und den Kantonen, Gutachten vom 22. Dezember 2011, JAAC 2012.1 (p. 1 - 17), édition du 1er mai 2012, p. 8; Lendi, Martin, in St. Galler Kommentar, 2e éd.. 2008, art. 81 N. 6

42 Ibid; Biaggini, Giovanni in BV-Kommentar, Zürich 2007, art. 81 N 2, critiqué par Markus Kern im Basler Kommentar, N 6 et 9.

d'édicter et d'imposer des normes techniques et organisationnelles contraignantes pour une collaboration TIC entre la Confédération et les cantons.[43]

6.2 Compatibilité avec les obligations internationales

L'avant-projet de loi est compatible avec les obligations internationales en vigueur. Lors de son élaboration, le Conseil fédéral s'est efforcé de ne pas exclure la possibilité d'assurer l'interopérabilité internationale. Si cela est souhaité ultérieurement, les e-ID reconnues en Suisse pourront obtenir la reconnaissance internationale. À cet effet, la conclusion d'accords internationaux sera nécessaire.

6.3 Forme de l'acte à adopter

Au vu de l'objet, du contenu et de la portée du projet, il est indispensable, selon l'art. 164, al. 1, Cst., d'édicter les dispositions relatives aux moyens de preuve électroniques sous la forme d'une loi fédérale.

À la demande du milieu politique, l'avant-projet de loi a été élaboré sous une forte pression du temps. Il est également très abstrait en raison de sa neutralité technologique et il avance sur un terrain nouveau avec la création d'une infrastructure publique immatérielle de la Confédération (cf. art. 81 Cst.). Il conviendra de l'adapter en fonction des résultats de la consultation, notamment en ce qui concerne l'expérience acquise lors des essais pilotes et l'utilisation sectorielle envisagée par les autorités publiques.

6.4 Frein aux dépenses

Comme le projet entraîne des dépenses périodiques de plus de 2 millions de francs, il doit être adopté à la majorité des membres de chaque conseil, conformément à l'art. 159, al. 3, let. b, Cst.

6.5 Respect du principe de la subsidiarité et du principe de l'équivalence fiscale

L'opportunité d'instaurer les e-ID et l'infrastructure de confiance est un point incontesté. Ni le partage des tâches prévu, ni leur exécution ne violent le principe de la subsidiarité ni celui de l'équivalence fiscale. Les conséquences financières du projet pour la Confédération sont supérieures à 10 millions de francs. Les conséquences financières pour les cantons dépendent ne sont pas encore chiffrables.

6.6 Délégations de compétences législatives

L'avant-projet de loi ne contient pas de délégations de compétences législatives. Aux art. 6, 11, al. 4, 25, 26 et 27, le Conseil fédéral se voit simplement confier la compétence d'édicter du droit réglementaire destiné à permettre l'application de la loi.

6.7 Protection des données

Les dispositions du droit de la protection des données (nLPD et ordonnances associées) s'appliquent à toutes les parties impliquées. Les particuliers, les émetteurs et les vérificateurs du secteur privé sont soumis aux dispositions applicables aux personnes privées; la Confédération (fedpol et autres autorités), les émetteurs et les vérificateurs du secteur public sont soumis dispositions applicables aux organes fédéraux. Le présent avant-projet de loi ne renvoie pas aux dispositions pertinentes de la nLPD afin d'éviter des répétitions et d'assurer une clarté lors de l'interprétation.

La protection des données est un des buts de l'avant-projet de loi, dans son champ d'application. L'art. 1, al. 2 reprend d'ailleurs le but fixé à l'art. 6 nLPD et précise également aux ch. 1 à 4 comment il sera mis en œuvre dans le contexte de l'e-ID. Il s'agit notamment d'intégrer les exigences des six motions de même teneur intitulées « À l'État de mettre en place une identification électronique fiable » (cf. 21.3124, 21.3125, 21.3126, 21.3127, 21.3128 et 21.3129) qui ont été déposées par tous les groupes parlementaires qui ont été soumises suite au rejet de l'ancien projet de loi lors de la votation du 7 mars 2021. Les motionnaires ont demandé l'identité électronique étatique respecte certains principes: prendre en compte la protection de la vie privée dès la conception du produit (*privacy by design*), ne collecter que les données nécessaires et enregistrer celles-ci de manière décentralisée (par exemple auprès de l'utilisateur en ce qui concerne les données d'identification). L'art. 1, al. 2, let. b lettre reformule ces exigences en tant que buts spécifiques à atteindre dans le cadre de la protection des données personnelles.

En outre, l'art. 1, al. 2, let. c de l'avant-projet de loi vise à garantir que la conception de l'E-ID et de l'infrastructure de confiance corresponde à l'état actuel de la technique. La notion « d'état actuel de la technique » se distingue conceptuellement des autres états technologiques similaires tels que les « les règles reconnues de la technique » et « l'état de la science et de la recherche ». En termes simples, le terme « état actuel de la technique » est plus innovant que le terme « règles reconnues de la technique » et plus obsolète que le terme « l'état de la science et de la recherche ». Cette distinction est la base essentielle pour déterminer le niveau de sécurité exigé. L'art. 7, al. 2 nLPD exige également la prise de mesures qui correspondent à « l'état de la technique », mais n'établit pas des critères pour déterminer ce qu'il faut entendre par « l'état de la technique ». Ce fait ne doit toutefois pas mener à la conclusion que ce qui n'est pas défini concrètement dans la loi ne peut pas être vérifié et par conséquent, ne peut pas être appliqué. Le législateur vise avec l'emploi de ce terme un niveau élevé de sécurité et de protection des données grâce à des procédures avancées. À cet

[43] Ibid; Biaggini, G., ibid, art. 81 N 3

effet, il convient d'encourager l'examen régulier des mesures de sécurité mises en œuvre quant à leur efficacité par rapport aux objectifs de protection requis, leur actualité et leur degré d'innovation. Il en résulte également une comparaison des mesures de sécurité avec les produits de sécurité existants sur le marché : Ce qui est considéré aujourd'hui comme correspondant à « l'état de la technique » peut être considéré demain en raison du décalage dû à l'innovation, c'est-à-dire de l'obsolescence de la mesure de sécurité par rapport à des autres mesures de sécurité disponibles, comme une des « règles reconnues de la technique ».

Pour des raisons de transparence, l'art. 2 énumère les données qui feront partie d'une e-ID. Il s'agit des données d'identification personnelles de base (al. 2) et des données supplémentaires (al. 3). Les données d'identification personnelles de base du titulaire sont les suivantes: le nom officiel, les prénoms, la date de naissance, le genre, le lieu de naissance, la nationalité et la photographie enregistrée dans ISA et SYMIC. Il s'agit de données disponibles dans les registres officiels de l'Etat auxquels fedpol à accès selon l'art 11, al. 3. En sus des données d'identification personnelles de base, une e-ID contient le numéro AVS et des données supplémentaires créées par fedpol lors de l'émission de l'e-ID : Il s'agit du numéro de l'e-ID, de la date d'émission, de la date d'expiration, et des données relatives au processus d'émission. En outre, l'e-ID contient les données relatives au document d'identité utilisé pour émettre l'e-ID, en particulier en ce qui concerne le type, le numéro et la durée de validité du document d'identité. Les détails seront précisés par voie d'ordonnance.

En vertu de l'art. 34, al. 1, nLPD, un organe fédéral n'est en droit de traiter et de communiquer des données personnelles que s'il existe une base légale. En application de l'art. 6, al. 3, nLPD, il y a lieu de définir la finalité du système envisagé de manière précise et reconnaissable pour les personnes concernées. Ainsi, la présente loi prévoit des règles précises permettant à fedpol de gérer un système d'information pour l'identification des requérants. L'art. 11 définit la nature, le contenu et la finalité de ce système. L'art. 11, al. 2, énumère les types de données qui y sont enregistrées: les données supplémentaires visées à l'art. 2, al. 3 ainsi que les données liées à la révocation d'une e-ID. En outre, on y conserve également les données, dites secondaires, créés durant le processus de vérification de l'identité et d'émission de l'e-ID, qui sont requises à des fins d'analyse statistique, d'assistance et de prévention d'abus. Les données personnelles sont consultées directement dans les registres fédéraux et ne sont pas sauvegardées dans le système d'information de fedpol (cf. al. 3). L'art. 11, al. 3 énumère les registres fédéraux auxquels fedpol aura accès afin de mettre en concordance les données personnelles. La finalité du système envisagé est de permettre à fedpol d'accomplir ses tâches dans le cadre de l'émission et de la révocation des moyens d'identification électronique. En outre, l'al. 4 fixe une limite de 5 ans pour la conservation des données dans le système suivant l'expiration de l'e-ID. Le Conseil fédéral se voit déléguer la compétence de régler par voie d'ordonnance les délais de conservation des différents types de données.

L'infrastructure de confiance mise en place par l'avant-projet de loi se fonde sur le principe de minimisation des données, de protection de la vie privée dès la conception et par défaut et d'enregistrement décentralisé des données. Les composants principaux de cette infrastructure sont réglés à la section 5. Il s'agit du registre de base, du mécanisme de confirmation des identifiants et de l'application pour la conservation et la présentation des moyens de preuve électroniques. Le registre de base et le système de confirmation des identifiants ne contiennent de trace des moyens de preuves électroniques. Seul le registre de base contient des informations liées à leur révocation. Les données des titulaires de l'e-ID et des moyens de preuve électroniques ne sont uniquement communiqué entre l'émetteur, le titulaire et des vérificateurs sans intermédiaire. Une base légale au sens de l'art. 34, al. 1, nLPD n'est donc pas requise. Le concept au cœur de l'infrastructure de confiance vise à créer un système dans lequel les flux de données sont directs et transparents pour tous les utilisateurs, où les émetteurs ne savent pas comment les moyens de preuve électroniques émis sont utilisées sans perdre le droit de les révoquer et dans lequel les titulaires profitent des mesures de sécurité correspondant à l'état actuel de la technologie.

Enfin, le Conseil fédéral se voit également déléguer à l'art. 28, let. e la compétence de régler par voie d'ordonnance les les mesures techniques et organisationnelles à prendre pour garantir la protection et la sécurité des données lors de l'exploitation et de l'utilisation de l'infrastructure de confiance.