Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

23.073

Message concernant la loi fédérale sur l'identité électronique et d'autres moyens de preuves électroniques

du 22 novembre 2023

Monsieur le Président,
Madame la Présidente,
Mesdames, Messieurs,

Par le présent message, nous vous soumettons les projets d'une la loi fédérale sur l'identité électronique et d'autres moyens de preuves électroniques et d'un arrêté fédéral sur les crédits d'engagement alloués à la mise en place et à l'exploitation de l'e-ID, en vous proposant de les adopter.

Nous vous proposons simultanément de classer les interventions parlementaires suivantes:

2021 M 21.3124 À l'État de mettre en place une identification électronique fiable (N 14.9.21; E 13.6.22)

2021 M 21.3125 À l'État de mettre en place une identification électronique fiable (N 14.9.21; E 13.6.22)

2021 M 21.3126 À l'État de mettre en place une identification électronique fiable (N 14.9.21; E 13.6.22)

2021 M 21.3127 À l'État de mettre en place une identification électronique fiable (N 14.9.21; E 13.6.22)

2021 M 21.3128 À l'État de mettre en place une identification électronique fiable (N 14.9.21; E 13.6.22)

2021 M 21.3129 À l'État de mettre en place une identification électronique fiable (N 14.9.21; E 13.6.22)

Nous vous prions d’agréer, Monsieur le Président, Madame la Présidente, Mesdames, Messieurs, l’assurance de notre haute considération.

22 novembre 2023

Au nom du Conseil fédéral suisse:

Le président de la Confédération, Alain Berset
Le chancelier de la Confédération, Walter Thurnherr

Condensé

Une nouvelle identité électronique (e-ID), gratuite et facultative, permettra de prouver son identité par des moyens numériques, de manière simple, sûre et rapide. Émise par la Confédération, elle garantira le plus grand degré possible de protection des données personnelles. Les titulaires auront la maîtrise la plus vaste possible de leurs données. L'infrastructure de confiance mise en place par la Confédération pour gérer les e-ID pourra également être utilisée par d'autres autorités et par les acteurs du secteur privé qui souhaitent établir et vérifier des moyens de preuves électroniques.

Contexte

Après le rejet par le peuple de la loi fédérale sur les services d'identification électronique, le 7 mars 2021, le Conseil fédéral a chargé le Département fédéral de justice et police d'esquisser une solution d'identification électronique étatique, en collaboration avec la Chancellerie fédérale et le Département fédéral des finances. Entretemps, le Conseil national et le Conseil des États ont approuvé six motions identiques, émanant de tous les groupes parlementaires et demandant la mise en place d'un système géré par l'État qui permette de prouver son identité en ligne.

Soucieux d'associer très tôt les milieux intéressés à l'élaboration de la nouvelle loi, l'Office fédéral de la justice a mené une consultation publique informelle à l'automne 2021. En se fondant sur les avis reçus, le Conseil fédéral, le 17 décembre 2021, a pris une décision de principe dans laquelle il a jeté les fondements de la future e-ID. Le projet de loi a été mis en consultation du 29 juin 2022 au 20 octobre 2022.

Contenu du projet

La nouvelle e-ID permet de s'identifier par des moyens numériques de manière simple, sûre et rapide. Tout titulaire d'une carte d'identité suisse, d'un passeport suisse ou d'un titre de séjour peut en demander une. La Confédération fournit une application pour téléphone portable dans laquelle l'utilisateur peut gérer son e-ID en toute sécurité. L'e-ID peut être utilisée aussi bien sur Internet (par ex. pour commander en ligne un extrait du casier judiciaire) que dans le monde réel (par ex. pour prouver son âge lors de l'achat d'alcool). Contrairement à ce que prévoyait la loi rejetée en votation, la Confédération émet les e-ID et exploite l'infrastructure nécessaire.

Les titulaires de l'e-ID ont la maîtrise la plus vaste possible de leurs données (identité souveraine ou self-sovereign identity). La protection des données est assurée par le système lui-même (principe de la protection des données dès la conception et par défaut), comme le demandent les motions déposées, mais aussi par la limitation des flux de données nécessaires (principe de la minimisation des données) et par l'enregistrement décentralisé des données. Par ailleurs, le Conseil fédéral a formulé le texte de loi de manière la plus neutre possible sur le plan technologique, afin que le système puisse toujours rester conforme au dernier état de la technique. En tout état de cause, le système suisse d'identification électronique respecte les normes internationales afin que l'e-ID puisse être reconnue et utilisée à l'étranger.

L'utilisation d'une e-ID est gratuite et facultative. L'identification physique sur place reste possible, même si l'utilisation de l'e-ID est également prévue. Par ailleurs, toutes les autorités, y compris cantonales et communales, doivent accepter l'e-ID lorsqu'elles recourent à l'identification électronique, par exemple au moment de délivrer une attestation de domicile ou un extrait du registre des poursuites.

L'infrastructure de confiance mise en place par la Confédération pour gérer les e-ID peut également être utilisée par les autorités cantonales et communales et par les acteurs du secteur privé qui souhaitent établir des moyens de preuves électroniques. Ainsi, les documents officiels, tels que les attestations de domicile ou les extraits du registre des poursuites, mais aussi les diplômes, les billets de concert ou les cartes de membre, peuvent être émis sous forme numérique à l'aide de l'infrastructure de confiance de l'État, puis enregistrés et gérés en toute sécurité dans l'application fournie par la Confédération ou dans une application de son choix.

Un arrêté fédéral sur les crédits d'engagement alloués à la mise en place et à l'exploitation de l'e-ID est également soumis au Parlement. Un crédit supplémentaire de 15,3 millions de francs ainsi que deux autres crédits d'engagement d'un montant total de 85,1 millions de francs sont proposés.

Table des matières

Message

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» (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 adoptées par le Conseil national le 14 septembre 2021 et par le Conseil des États le 13 juin 2022. La discussion relative à l'interpellation 21.3310 Andrey a été reportée et classée le 17 mars 2023. En outre, le Conseil national a décidé de liquider l'interpellation 21.3718 Graf-Litscher.

Lors de sa séance du 26 mai 2021, le Conseil fédéral a déclaré qu'il souhaitait présenter rapidement une nouvelle solution pour l'identification électronique, qui tienne compte des préoccupations des auteurs des motions. Il a ainsi chargé le Département fédéral de justice et police (DFJP) de rédiger, avant la fin 2021, une ébauche de texte en collaboration avec le Département fédéral des finances (DFF) et la Chancellerie fédérale (ChF) et en lien étroit avec les cantons et les deux Écoles polytechniques fédérales de Zurich et Lausanne. Il s'agissait en particulier d'examiner les différentes possibilités techniques de réalisation de l'e-ID et de préciser leurs dépenses respectives.

Le DFJP a préparé un document de travail concernant le projet d'identité électronique (e-ID)[1] (ci-après «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 (ICP) et le fournisseur d'identité central étatique (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. 60 avis ont été soumis par des administrations cantonales ainsi que des représentants des milieux scientifiques, des organisations économiques et des entreprises[2]. 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 infor-

1 www.admin.ch > État & Citoyen > Projets législatifs en cours e-ID étatique > Document de travail concernant le projet d'identité électronique (e-ID)

2 www.bj.admin.ch > État & Citoyen > Projets législatifs en cours > e-ID étatique > Rapport sur les résultats de la consultation publique concernant le projet d'identité électronique (e-ID)

melle était 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 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 six motions déposées à la suite de la votation. Dans le cadre de futurs travaux, il convient de prendre en considération cette volonté ainsi que les principes du respect de la vie privée dès la conception, 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 poursuivrait une approche fondée sur les principes du respect de la vie privée dès la conception, de l'économie des données et de l'enregistrement décentralisé des données et s'appuyant sur une infrastructure de confiance étatique permettant de mettre en place un écosystème de moyens de preuves électroniques émis par les acteurs des secteurs public et privé. 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.

L'avant-projet de loi a été mis en consultation du 29 juin au 20 octobre 2022. Au total, 117 avis ont été exprimés, dont la majorité positifs. En particulier, la nouvelle distribution des rôles, avec l'État comme émetteur de l'identité électronique et exploitant de l'infrastructure de confiance sur laquelle elle repose, a été saluée. Les réponses font apparaître une claire volonté d'aboutir à une solution stable, sûre et facile d'utilisation. Sur la base des résultats de la consultation, le Conseil fédéral a élaboré le présent projet de loi.

1.1 Relation avec le programme de la législature et avec le plan financier, ainsi qu'avec les stratégies du Conseil fédéral

Le projet de 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[3] et dans l'arrêté fédéral du 14 juin 2016 sur le programme de la législature 2015 à 2019[4]. Après son rejet lors de la votation du 7 mars 2021, le Conseil fédéral a décidé de relancer et de réorienter les travaux législatifs en matière

3 FF **2016** 981, 1048 et 1100
4 FF **2016** 4999, 5001

d'identité électronique. Le projet n'a pas été annoncé à nouveau dans le message du 29 janvier 2020 sur le programme de la législature 2019 à 2023[5], ni dans l'arrêté fédéral du 21 septembre 2020 sur le programme de législature 2019 à 2023[6].

1.2 Classement d'interventions parlementaires

Le projet de loi proposé met en œuvre les interventions parlementaires suivantes:

– Motions issues 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, ne collecter que les données nécessaires et enregistrer celles-ci de manière décentralisée (par ex. auprès de l'utilisateur en ce qui concerne les données d'identification). Les motions ont été adoptées le 14 septembre 2021 par le Conseil national, et le 13 juin 2022 par le Conseil des États, conformément à la proposition du Conseil fédéral.

Lors de l'élaboration du projet, 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. Le 17 mars 2023, l'interpellation a été classée car le Conseil national n'a pas achevé son examen dans un délai de deux ans.

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

2 Procédure préliminaire, consultation comprise

2.1 La première loi fédérale sur les services d'identification électronique

Les travaux législatifs relatifs à l'e-ID ont débuté en 2013. Le 27 septembre 2019, le Parlement a adopté à une large majorité la loi fédérale sur les services d'identification électronique (LSIE). Cette loi prévoyait que l'e-ID serait délivrée par des fournisseurs d'identité appartenant au secteur privé, sur la base des données d'identité que leur communiqueraient l'Office fédéral de la police (fedpol). La Confédération n'aurait établi elle-même des e-ID qu'à défaut de fournisseurs privés. Suite à une demande de référendum, la LSIE a été rejetée par le peuple le 7 mars 2021, à une nette majorité. L'analyse VOX du résultat de cette votation a toutefois montré que la majorité des

5 FF **2020** 1709
6 FF **2020** 8087

votants n'était pas opposée à l'identification électronique en soi, mais au fait que l'e-ID soit établie par des fournisseurs privés.

2.2 Le «document de travail concernant le projet d'identité électronique (e-ID)»

Quelques jours après le rejet de la LSIE, le 10 mars 2021, six motions identiques ont été déposées (voir ch. 1.2). Elles fixent les objectifs principaux de la future e-ID, mais sans préciser comment elle doit être conçue pour les atteindre. Comme une procédure de consultation ordinaire ne se prête guère à faire un choix entre les grandes orientations possibles du projet, la cheffe du DFJP a ouvert une consultation publique informelle, le 2 septembre 2021, à l'occasion de la réunion d'un comité consultatif.

Le document de travail concernant le projet d'identité électronique (e-ID) soumis à cette consultation fait un état des lieux des solutions possibles. Il présente plusieurs définitions et plusieurs dimensionnements possibles de la future e-ID en Suisse et de l'infrastructure dans laquelle celle-ci devra s'inscrire. Il expose en outre trois approches technologiques pour la réaliser:

- l'identité souveraine (SSI)
- l'infrastructure à clef publique (ICP)
- le fournisseur d'identité central étatique.

Une majorité des participants à cette consultation a estimé que l'identité souveraine était le moyen technologique le plus approprié pour répondre aux exigences en matière de valeurs et de fonctions. Quelques-uns seulement privilégient l'infrastructure à clef publique ou le fournisseur d'identité central, principalement parce que ces solutions sont connues de longue date.

À la question de savoir s'il fallait, pour la sécurité, basculer sur l'utilisation d'un *hard token* (appareil ou boîtier pour la conservation de clefs numériques privées), une majorité a clairement répondu non, invoquant la facilité d'utilisation, alors qu'un tout petit nombre de participants estiment qu'un module de sécurité matériel est quasi indispensable à une e-ID sécurisée.

Outre l'approche technologique, le document de travail proposait trois «niveaux d'ambition» (c'est-à-dire trois possibilités pour le futur champ d'application de l'e-ID), en s'inspirant des débats en cours dans l'UE:

- Niveau d'ambition 1: l'e-ID est la seule preuve numérique disponible.
- Niveau d'ambition 2: outre l'e-ID, l'État peut émettre d'autres preuves numériques.
- Niveau d'ambition 3: tant des services publics que privés peuvent émettre d'autres preuves numériques que l'e-ID.

Presque tous les participants ayant exprimé une opinion sur ce point ont mentionné le niveau d'ambition 3 comme objectif à atteindre. Une progression du niveau d'ambition 1 au 2 puis au 3 est tout à fait envisageable pour certains.

La consultation s'est achevée par un débat public sous forme de conférence le 14 octobre 2021.

2.3 La décision de principe du Conseil fédéral

Se fondant sur les résultats de la consultation informelle sur le document de travail concernant le projet d'identité électronique, le Conseil fédéral a fixé le 17 décembre 2021 les grandes lignes de la future preuve d'identité numérique émise par l'État: les utilisateurs de l'e-ID devront, dans toute la mesure du possible, être maîtres de leurs données (principe de l'identité 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 par la sauvegarde décentralisée des données. L'e-ID reposera sur une infrastructure gérée par l'État, qui pourrait être mise à la disposition de services publics ou privés, qui s'en serviraient pour émettre toutes sortes de preuves numériques (écosystème e-ID du niveau d'ambition 3).

2.4 Aperçu des résultats de la procédure de consultation

Une procédure de consultation sur un avant-projet de (deuxième) loi sur l'e-ID a eu lieu du 29 juin au 20 octobre 2022. Au total, 117 participants se sont prononcés.

2.4.1 Remarques générales

Les réactions au nouvel avant-projet sont majoritairement positives. La nouvelle répartition des rôles, notamment, qui fait de l'État l'émetteur de l'identité électronique et l'exploitant de l'infrastructure de confiance nécessaire, suscite une large adhésion. Dans l'ensemble, les participants appellent clairement de leurs vœux la mise en place rapide d'une solution stable, sûre et conviviale. Ils se félicitent par ailleurs de la rapidité avec laquelle l'avant-projet a été élaboré, de la transparence de la procédure et de son caractère participatif.

Trois d'entre eux rejettent résolument l'avant-projet: l'UDC pour cause, dit-elle, d'absence de base constitutionnelle claire, le conseiller à la protection des données du canton du Tessin et le Parti pirate pour des questions de protection des données, le Parti pirate invoquant des motifs supplémentaires.

2.4.2 Remarques concernant la notion d'identité électronique souveraine et le rôle de l'État

Les avis exprimés ne s'inquiètent plus du rôle de l'État que de façon marginale – contrairement à ce qui avait été le cas pour la première loi rejetée en votation populaire, selon laquelle l'e-ID était émise par des acteurs du secteur privé. Personne ne

conteste que l'État doit être le responsable du développement et de l'exploitation de l'infrastructure de confiance et l'unique émetteur de l'identité électronique étatique.

Les participants à la consultation reconnaissent les avantages du concept d'identité électronique souveraine, qui permet de mettre en œuvre les principes de la protection des données dès la conception, de l'économie des données et de l'enregistrement décentralisé des données. Ils sont par ailleurs nombreux à apprécier le fait que les personnes privées pourront elles aussi utiliser l'infrastructure de confiance.

2.4.3 Autres points

Plusieurs questions ont été soulevées lors de la consultation:

- Certains demandent un élargissement du cercle des personnes habilitées à demander une e-ID, d'autres exigent qu'il soit limité afin de garantir que seules les personnes dont l'identité peut être constatée de manière fiable recevront une e-ID.
- Les participants ont formulé un grand nombre de requêtes concernant la procédure d'émission de l'e-ID, dont la principale est de doubler la procédure en ligne d'une procédure au guichet.
- La protection des données occupe naturellement une place centrale dans la plupart des avis exprimés. Nombre de participants sont favorables à son renforcement, notamment face au risque que certains vérificateurs exigent une e-ID sans motif valable ou exigent plus que les éléments minimaux requis de l'e-ID.
- L'avant-projet ne traite pas de l'accessibilité aux personnes handicapées car il s'agit là d'une obligation légale systématique de la Confédération. Bon nombre de participants souhaitent néanmoins que cet aspect soit expressément réglé dans la LeID.
- L'avant-projet prévoit que les cantons désigneront des points de contact chargés d'offrir une assistance en relation avec l'émission et l'utilisation des e-ID. Alors que nul ne conteste la nécessité d'une assistance, bon nombre de participants appellent la Confédération à s'investir plus activement en proposant un service d'assistance central. Les cantons se considèrent surtout comme compétents pour guider les utilisateurs de l'e-ID dans la cyberadministration.

2.5 Appréciation des résultats de la consultation

Contrairement à l'argumentation de l'UDC, le Conseil fédéral estime que la loi sur l'identité électronique repose sur une base constitutionnelle solide (cf. ch. 7.1). Les réserves exprimées par le préposé à la protection des données du canton du Tessin et par le Parti pirate en matière de protection des données sont compréhensibles mais insuffisantes pour justifier un rejet de l'avant-projet de la loi (cf. ch. 7.7).

Parmi les avis exprimés lors de la consultation externe, les propositions suivantes ont été intégrées en particulier dans le projet de loi:

- il sera possible d'obtenir l'e-ID non seulement en ligne mais aussi au guichet;
- des restrictions seront mises en place pour empêcher la demande de données qui ne sont pas nécessaires à l'obtention de la prestation demandée, et des sanctions seront prévues;
- l'accessibilité aux personnes handicapées sera réglée explicitement;
- l'assistance aux utilisateurs pour l'émission de l'e-ID et l'utilisation de l'infrastructure de confiance sera confiée à fedpol et à l'Office fédéral de l'informatique et de la télécommunication (OFIT), en lieu et place des points de contact cantonaux prévus dans l'avant-projet.

3 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 (UE). 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[7] visant à modifier le règlement (UE) nº 910/2014[8] (règlement eIDAS) et à établir un cadre juridique pour une identité électronique européenne. Dans le cadre du nouveau règlement, il est prévu que les États membres offriront aux citoyens et aux entreprises, dans les douze 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.

Le 6 décembre 2022, le Conseil a adopté son orientation générale concernant le cadre pour une identité numérique européenne. Au Parlement européen, le dossier a été confié à la commission de l'industrie, de la recherche et de l'énergie (ITRE). Le Parlement a adopté sa position le 16 mars 2023, et les négociations ont commencé par la suite. 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 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 10 février 2023, la Commission a publié la première version d'une boîte à outils commune de l'UE pour

7 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.

8 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.

mettre en œuvre le portefeuille européen d'identité numérique (portefeuille EUDI)[9]. 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 eIDAS 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'UE, elle a tout intérêt à rendre son système d'identité électronique interopérable avec celui de cette dernière. Le 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. 31). Il sera ainsi possible d'obtenir une reconnaissance mutuelle, notamment avec l'UE. Le projet de loi a été formulé de manière à être compatible avec le droit européen en la matière.

4 Présentation du projet

4.1 Réglementation proposée

Le 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. Comme le demandent les motions déposées au Conseil national, le nouveau projet poursuit une approche fondée sur les principes du respect de la vie privée dès la conception et par défaut, de l'économie des données et de l'enregistrement décentralisé des données.

En outre, le 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 preuves électroniques. Dans ce cadre, l'État exploitera les systèmes de base nécessaires (registre de base, registre de confiance) et offrira un portefeuille électronique étatique sous forme d'application mobile, qui pourra contenir l'e-ID et d'autres moyens de preuves électroniques. Les titulaires du portefeuille pourront présenter leur e-ID et autres moyens de preuves électroniques de manière sécurisée et transparente. Une telle ouverture du système permettra d'améliorer la diffusion et d'augmenter l'utilisation des moyens de preuves électroniques. En même temps, elle permettra de renforcer le niveau de confiance dont bénéficient les processus électroniques au sein de la population. Des applications alternatives pour la conservation et la présentation de moyens de preuves électroniques (porte-monnaie électroniques) pourront être utilisées, dans la mesure où elles sont compatibles du point de vue technique.

La mise en place par l'État d'une infrastructure électronique de confiance est un développement important et innovant. En outre, ce projet se fonde sur une procédure

9 Boîte à outils commune de l'Union pour une approche coordonnée en vue d'un cadre européen relatif à une identité numérique: Architecture du portefeuille européen d'identité numérique et cadre de référence, janvier 2023, version 1.0.0 (en anglais).

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 de l'utilisation de l'e-ID dans divers domaines n'est réglée qu'à titre indicatif dans le projet de loi (cf. modification d'autres actes législatifs: loi fédérale du 11 avril 1889 sur la poursuite pour dettes et la faillite [LP][10] et loi fédérale du 19 juin 2015 sur le dossier électronique du patient [LDEP][11]). Ce point a été examiné lors de la consultation. Au vu de la grande diversité des cas de figure possibles, il convient de régler l'utilisation de l'e-ID dans les lois applicables aux domaines pertinents.

4.2 Adéquation des moyens requis

Une estimation des dépenses a été réalisée (cf. ch. 6.1, Conséquences sur les finances et l'état du personnel pour la Confédération).

Au total, les moyens financiers nécessaires pour le développement et l'exploitation de l'infrastructure de confiance, l'émission des e-ID et les projets pilote seront d'environ 181,9 millions de francs sur la période 2023 à 2028. A partir de 2029, il faut s'attendre à des dépenses avoisinant les 24,7 millions de francs par an.

Ces besoins financiers peuvent être qualifiés de raisonnables pour un projet de cette importance, et qui servira de base pour faire avancer la numérisation en Suisse.

4.3 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. 28 et les commentaires s'y rapportant).

5 Commentaire des dispositions

Préambule

Le projet de loi se fonde sur les art. 38, al. 1, 81, et 121, al. 1, de la Constitution (Cst.)[12].

S'agissant de l'identité électronique étatique, le projet de loi repose sur les art. 38, al. 1, et 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

10 RS **281.1**
11 RS **816.1**
12 RS **101**

pas expressément les documents d'identité, il est possible de déduire de ces normes de délégation que la Confédération a 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 du 22 juin 2001 sur les documents d'identité (LDI)[13] et loi fédérale du 16 décembre 2005 sur les étrangers et l'intégration (LEI)[14] permettent à la Confédération d'émettre des documents d'identité pour les citoyens suisses et des permis pour les étrangers. Comme l'e-ID étatique sert à prouver l'identité dans le monde virtuel et que le droit d'obtenir une e-ID est étroitement lié au droit d'obtenir le document physique correspondant, il est justifié de fonder le présent 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 cependant se fonder sur une autre compétence fédérale. Un «ouvrage» ou des «travaux publics» visés par cette disposition sont traditionnellement de nature physique, au sens d'une construction, par exemple un tunnel. Toutefois, selon l'avis de droit de l'Office fédéral de la justice (OFJ) concernant la coopération TIC entre la Confédération et les cantons[15], il serait possible, selon une approche partiellement soutenue par la doctrine, d'inclure dans la notion de «travaux» de l'art. 81 Cst. les grands projets informatiques et autres éléments visant à créer un paysage administratif électronique uniforme[16]. En effet, suivant l'interprétation évolutive et téléologique de Lendi[17] et de Biaggini[18], 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 projet de loi qui vise à mettre en place une infrastructure de confiance permettant d'émettre, d'utiliser et de valider divers moyens de preuves 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 des normes techniques et organisationnelles contraignantes pour une collaboration TIC entre la Confédération et les cantons[19]. Par contre, la Confédération peut édicter les

13 RS **143.1**
14 RS **142.20**
15 DFJP, Office fédéral de la justice, Rechtsgrundlagen für die IKT-Zusammenarbeit zwischen dem Bund und den Kantonen, Gutachten vom 22. Dezember 2011, JAAC 2012.1 (p. 1 à 17), édition du 1er mai 2012.
16 *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».*
17 *Ibid*; Lendi, Martin, in St. Galler Kommentar, 2e éd. 2008, art. 81 N 6; Vogel, Stefan, in St. Galler Kommentar, 4e éd. 2023, art. 81 N 5.
18 *Ibid*; Biaggini, Giovanni in BV-Kommentar, Zurich 2007, art. 81 N 2, critiqué par Markus Kern in Basler Kommentar, N 6 et 9.
19 *Ibid*; Biaggini, G., *ibid*, art. 81 N 3.

règles nécessaires à la mise à disposition et à l'utilisation sûres, efficaces et uniformes des travaux ou ouvrages publics en question.

Le présent 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

Let. a

Le projet de loi règle les exigences relatives à l'infrastructure de confiance servant à l'émission, à la révocation, au contrôle, à la conservation et à la présentation des moyens de preuves électroniques.

Let. b

Le projet de loi règle les rôles et les responsabilités relatifs à la mise à disposition et à l'utilisation de l'infrastructure de confiance.

Let. c

Le projet de loi établit le cadre juridique des moyens de preuves électroniques en Suisse, y compris l'identité électronique étatique.

Al. 2

Let. a

Le texte de la let. a a été remanié afin de tenir compte des résultats de la consultation. Plusieurs participants ont critiqué le fait que la disposition ne reprenait que partiellement le principe de la protection des données dès la conception et par défaut prévu à l'art. 7 de la loi fédérale du 25 septembre 2020 sur la protection des données (LPD)[20]. Cette lettre a été reformulée sur la base du texte de l'art. 7, al. 2, LPD au lieu du principe plus général énoncé à l'art. 1 LPD. Son but est de garantir que les mesures techniques et organisationnelles prévues sont appropriées au regard notamment de l'état de la technique, du type de traitement des données et de son étendue, ainsi que du risque que ce traitement présente pour la personnalité ou les droits fondamentaux des personnes concernées.

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» (21.3124, 21.3125, 21.3126, 21.3127, 21.3128 et 21.3129) qui ont été déposées par des parlementaires issus de tous les groupes après le rejet de l'ancien projet

20 RS **235.1**

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, ne collecter que les données nécessaires et enregistrer celles-ci de manière décentralisée (par ex. auprès de l'utilisateur en ce qui concerne les données d'identification). La let. a reformule ces exigences en tant que buts spécifiques à atteindre dans le cadre de la protection des données personnelles.

La LPD s'applique au traitement de données personnelles effectué dans le cadre de la mise en œuvre de la loi. Afin d'éviter des répétitions et de faciliter la compréhension, les dispositions du projet de loi ne contient pas de renvois aux articles pertinents de la LPD (cf. ch. 7.8 Protection des données).

En outre, le droit cantonal de la protection des données s'applique en principe à l'utilisation de l'infrastructure de confiance par les autorités cantonales dans la mesure où le traitement des données est imputable aux autorités cantonales. C'est notamment le cas lorsque celles-ci établissent leurs propres moyens de preuves électroniques ou vérifient des preuves électroniques (y compris l'e-ID). Certaines dispositions de la présente loi interviennent toutefois ponctuellement dans le droit cantonal. Ainsi, ce dernier doit respecter les normes minimales (plus élevées) prévues dans le projet de loi au même titre que les utilisateurs privés de l'infrastructure de confiance.

Let. b

La let. b spécifie que la loi vise à permettre l'émission et l'utilisation des moyens de preuves électroniques à un groupe de personnes spécifique. Ces moyens de preuves pourront ainsi être émis et utilisés dans le cadre des relations entre personnes privées et entre personnes privées et autorités.

Le projet de loi vise à assurer la mise en place de processus sûrs dans le cadre de l'infrastructure de confiance. Les risques relatifs à l'émission, l'utilisation et la présentation des moyens de preuves électroniques devront être minimisés par la prise de mesures techniques et organisationnelles appropriées.

Let. c

La let. c vise à garantir que la conception de l'e-ID et de l'infrastructure de confiance correspondent 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 «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 «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, LPD 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 cette expression. Cela 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.

En utilisant cette notion, le législateur vise un niveau élevé de sécurité et de protection des données grâce à des procédures avancées. À 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. 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 d'autres mesures de sécurité disponibles, comme une des «règles reconnues de la technique».

Let. d

Le projet de loi vise également à assurer la sécurité de l'infrastructure et des processus d'émission et de vérification des autres moyens de preuves électroniques. Afin d'atteindre ces buts, il convient toutefois de ne pas limiter le progrès technique. Ainsi, le 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. Les titulaires ont alors un plus grand contrôle sur leurs données. 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 grands pas, il convient de s'assurer que le présent projet de loi pourra être mis en œuvre dans le contexte technologique qui se présentera après son entrée en vigueur et qui n'est pas encore connu actuellement.

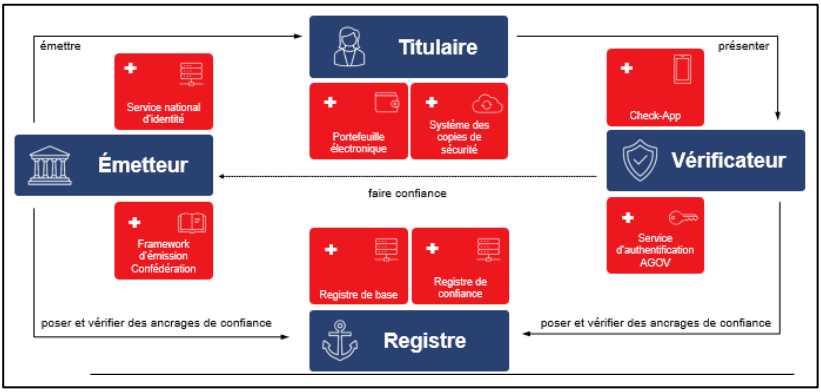
Différents aspects à régler au niveau de l'ordonnance seront beaucoup plus concrets et spécifiques sur le plan technologique. L'ordonnance devra garantir l'interopérabilité de tous les systèmes concernés par la communication. Pour ce faire, elle devra notamment définir très précisément les formats de 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 différents acteurs le choix de la technologie qu'ils entendent utiliser pour formater, stocker et traiter les données de leur côté de l'interface.

Section 2 Infrastructure de confiance

Le projet de loi donne à la Confédération la compétence de mettre en place, d'exploiter et de développer une infrastructure informatique permettant d'émettre, d'utiliser, de gérer, de valider et de révoquer des moyens de preuves électroniques. L'infrastructure de confiance met en œuvre un ensemble de règlements, de processus, de concepts et d'éléments d'infrastructure qui garantissent la conformité et la confiance du système conformément aux bonnes pratiques. L'infrastructure de confiance vise à permettre l'émission, la révocation et l'utilisation des e-ID et d'autres moyens de preuves électroniques.

Il existe trois types d'acteurs au sein de l'infrastructure de confiance: les émetteurs, les titulaires et les vérificateurs. Leurs interactions se fondent sur des normes de communication définies. L'infrastructure de confiance mise en place par la Confédération se compose des éléments suivants: le registre de base (art. 2), le registre de confiance

(art. 3), l'application pour la conservation et la présentation des moyens de preuves électroniques (art. 7) et l'application pour la vérification des moyens de preuves électroniques (art. 8). En plus, le système d'information (art. 25) et le service d'authentification de la Chancellerie fédérale (modification d'autres actes, loi fédérale du 17 mars 2023 sur l'utilisation des moyens électroniques pour l'exécution des tâches des autorités [LMETA][21]) avec l'e-ID complètent les éléments centraux prévus par le projet.



L'OFIT met en place et exploite les différents éléments de l'infrastructure de confiance. La responsabilité pour les dommages qui peuvent être causés lors de l'utilisation de l'e-ID ou de l'infrastructure de confiance est soumise aux règles de responsabilité usuelles du code des obligations[22] ou de la loi du 14 mars 1958 sur la responsabilité (LRCF)[23].

Art. 2 Registre de base

Al. 1

L'OFIT met un registre de base à la disposition des autorités et des personnes privées intéressées. Ce registre 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 s'assurer que les moyens de preuves électroniques n'ont pas été modifiés ultérieurement et qu'ils proviennent de l'émetteur inscrit dans le registre de base avec l'identifiant concerné.

Le registre de base peut être mis en place sous différentes formes. Toutefois, le choix de la solution technique n'est pas réglé par le projet de loi, qui demeure, dans la mesure du possible, technologiquement neutre (cf. commentaire de l'art. 1, al. 2, let. d). Ainsi, le projet de loi ne règle pas en détail les composants techniques du registre de base; il prévoit les fonctions que le registre de base devra remplir. À titre d'exemple,

21 FF **2023** 787
22 RS **220**
23 RS **170.32**

ce dernier pourra contenir les données suivantes: les identifiants des émetteurs et des vérificateurs; les clés cryptographiques requises pour contrôler leurs identifiants et pour vérifier l'authenticité et l'intégrité des moyens de preuves électroniques; les données relatives à la révocation des moyens de preuves électroniques. Les adresses, les numéros de téléphone, les adresses e-mail ou autres coordonnées des émetteurs et vérificateurs ainsi que les données personnelles des titulaires ne seront pas enregistrées dans le registre de base.

Al. 2

Les émetteurs peuvent inscrire eux-mêmes leurs données dans le registre de base, permettant ainsi à un vérificateur de contrôler l'authenticité (uniquement par rapport aux données que les émetteurs y ont inscrites) et l'intégrité des moyens de preuves électroniques émis par l'émetteur concerné. Ces données sont sécurisées par un algorithme cryptographique lors de l'inscription et sont considérées comme infalsifiables.

Les émetteurs et les vérificateurs voulant s'annoncer dans le registre de confiance visé à l'art. 3 doivent inscrire leurs informations dans le registre de base. A ce stade, leur identité n'est pas vérifiée. Une inscription dans le registre de base permet seulement de contrôler si certaines informations, telle qu'une clé publique, appartiennent à un identifiant donné, mais elle ne constitue pas une identité vérifiée. C'est le registre de confiance qui permet de confirmer l'appartenance d'un identifiant à un acteur (cf. commentaire de l'art. 3).

Al. 3

À l'exception des données concernant la révocation, le registre de base ne contient pas de données relatives aux moyens de preuves électroniques, telles les données personnelles relatives à l'émission des moyens de preuves électroniques.

Al. 4

Les données liées à la révocation des moyens de preuves électroniques ne permettent de tirer des conclusions ni sur l'identité du titulaire ni sur le contenu du moyen de preuve électronique.

Al. 5

La consultation a révélé que des exigences plus précises concernant l'utilisation des données personnelles générées lors de la consultation du registre de base étaient requises. Les données personnelles générées par la consultation du registre de base sont notamment des adresses IP, ou autres données similaires selon le protocole utilisé. L'al. 5 s'aligne sur l'art. 57*l*, let. b, ch. 1 à 3, de la loi du 21 mars 1997 sur l'organisation du gouvernement et de l'administration (LOGA)[24] d'un côté pour ce qui est des buts de l'enregistrement des données et d'un autre côté pour ce qui est des buts de l'analyse sans rapport avec des personnes de données personnelles. En outre, il prévoit que ces données peuvent être analysées en rapport avec des personnes mais de manière non nominale selon l'art 57*n*, let. a, LOGA et en rapport avec des personnes de manière nominale dans les buts prévus à l'Art. 57*o*, al. 1, let. a et b, LOGA.

24 RS **172.010**

Il convient de préciser que l'OFIT n'a pas accès au contenu des transactions entre les émetteurs, les titulaires et les vérificateurs.

Art. 3 Registre de confiance

Al. 1

L'OFIT met à disposition un système accessible au public (registre de confiance) qui contient des données pour la vérification de l'identité des émetteurs et des vérificateurs ainsi que pour l'utilisation sûre des moyens de preuves électroniques. Ce système 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. Au-delà de la vérification des identifiants, le système met également une multitude d'autres informations à la disposition des utilisateurs. Par exemple, il permet de vérifier si un émetteur est autorisé à émettre un certain type de moyen de preuve électronique (par ex. fedpol est le seul émetteur de l'e-ID) ou si un vérificateur peut exiger un moyen de preuve électronique particulier ou certaines informations qu'il contient (par ex. si un acteur peut demander le numéro AVS contenu dans l'e-ID).

Chaque acteur est libre de décider quand il consulte le registre de confiance. Le registre de confiance n'est pas requis pour la vérification cryptographique de moyens de preuves électroniques ou la création de canaux de communication sécurisés. Il peut néanmoins augmenter la confiance dont bénéficie un acteur auprès de son interlocuteur s'il n'y pas de relation existante entre les deux, si l'un des deux souhaite davantage d'informations ou si une confirmation de l'authenticité et de l'exactitude des informations partagées est requise.

Le registre de confiance est conçu de manière à pouvoir répondre à la fois aux demandes automatiques et aux demandes manuelles. Ce sont principalement les applications pour la conservation et la présentation (portefeuilles électroniques) et les systèmes utilisés par les vérificateurs qui auront recours à ces informations afin de mieux orienter les utilisateurs et de leur permettre de prendre des décisions éclairées.

Afin de minimiser le flux de données et de maintenir le caractère décentralisé de l'infrastructure de confiance, chaque confirmation du système peut être émise en tant que moyen de preuve électronique ou autre moyen similaire selon l'état de la technique. Ces moyens de preuves électroniques peuvent être présentés par un émetteur ou par un vérificateur à tout acteur intéressé et ne requièrent pas de consultation du registre de confiance par ce dernier. Il s'agit d'une option de mise en œuvre du registre de confiance, qui est en cours d'évaluation.

Al. 2

L'OFIT est responsable de l'exactitude des informations qui sont accessibles au public dans le registre de confiance. Il est chargé de mettre en place les processus nécessaires pour assurer la qualité et l'exactitude des informations et de les corriger ou de les mettre à jour, le cas échéant.

Al. 3

Afin de renforcer la confiance dont bénéficient les services cyberadministratifs recourant à l'infrastructure de confiance, les autorités fédérales, cantonales et communales sont inscrites au registre de confiance sur leur demande. Cette inscription confirme qu'un identifiant inscrit dans le registre de base leur appartient bien.

Al. 4

Le Conseil fédéral pourra prévoir que la Confédération confirme l'identifiant des émetteurs et des vérificateurs du secteur privé. Une telle mesure peut augmenter le niveau de confiance dont bénéficie l'infrastructure de confiance dans le contexte de l'identification électronique. Bien que les émetteurs et les vérificateurs du secteur privé soient intéressés en principe à utiliser le registre de confiance, il n'est pas certain qu'ils le feront vraiment une fois qu'il sera mis à disposition. Il faudra attendre l'entrée en vigueur du projet de loi afin de voir si ces intentions se concrétiseront.

Il conviendra alors de définir par voie d'ordonnance les exigences applicables à la confirmation de l'identifiant de ces entités. Il s'agira également de prévoir les mesures techniques et organisationnelles qui devront être prises pour assurer la qualité des informations mises à disposition par le registre de confiance.

Enfin, il est possible que les acteurs du secteur privé décident de mettre en place, à leur propre compte et séparément, des registres de confiance non étatiques (privés); le présent projet de loi ne leur impose pas de limitation dans ce domaine.

Al. 5

Cet alinéa vise à permettre aux utilisateurs de vérifier dans le registre de confiance si l'identifiant d'un émetteur ou d'un vérificateur a été confirmé par l'OFIT. Les confirmations des identifiants visées aux al. 3 et 4 doivent ainsi figurer au registre de confiance.

Al. 6

La consultation a révélé que des exigences plus précises concernant l'utilisation des données personnelles générées lors de la consultation du registre de confiance étaient requises. Les exigences sont les mêmes qu'à l'art. 2, al. 5; l'al. 6 renvoie donc à ce dernier, afin d'éviter des répétitions et de faciliter la lecture (cf. commentaire de l'art. 2, al. 5).

Ainsi, les données personnelles générées lors de la consultation du registre de confiance peuvent être enregistrées dans les buts prévus par l'art. 57*l*, let b, ch.1 à 3, LOGA. Elles peuvent être analysées sans rapport avec des personnes dans les buts prévus par l'art. 57*l*, let b, ch. 1 à 3, LOGA, en rapport avec des personnes mais de manière non nominale dans les buts prévus par l'art 57*n*, let. a, LOGA et en rapport avec des personnes de manière nominale dans les buts prévus à l'Art. 57*o*, al. 1, let. a et b, LOGA.

Al. 7

Cet alinéa délègue au Conseil fédéral la compétence de prévoir des règles sur la fourniture d'autres informations qui permettent de renforcer l'utilisation sûre des moyens

de preuves électroniques. Il pourra notamment s'agir de données qui indiquent comment les moyens de preuves électroniques sont utilisés ou de données qui permettent de savoir si un émetteur ou vérificateur est censé émettre ou vérifier un certain type de moyen de preuve électronique. Cette délégation de compétence permettra également au registre de confiance d'évoluer et de mieux répondre aux besoins de l'écosystème et du développement technique.

Art. 4 Émission

Al. 1

Toute autorité publique et toute personne privée peut utiliser l'infrastructure de confiance de la Confédération pour émettre des moyens de preuves 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 preuves électroniques qui peuvent être émis; il vise à ouvrir l'infrastructure de confiance à divers acteurs et à leur permettre d'émettre des moyens de preuves électroniques de toutes sortes.

Cette disposition est volontairement formulée de manière ouverte. Il ne s'agit notamment pas de limiter *a priori* le cercle des émetteurs ni le type de moyens de preuves électroniques. Pour la même raison, on a renoncé à prévoir des prescriptions concernant les informations que les émetteurs doivent conserver sur les moyens de preuves électroniques qu'ils ont délivrées. Ces décisions doivent être prises au cas par cas par les émetteurs eux-mêmes ou, dans le cas d'un émetteur public, par le législateur compétent.

L'al. 1 n'est pas potestatif pour l'OFIT, qui est chargé de mettre en place les différents composants de l'infrastructure de confiance selon les art. 2 et 3.

Al. 2

Les moyens de preuves électroniques sont composés de données diverses. En sus du contenu de base fixé par l'émetteur, ils doivent comprendre les données requises pour la vérification de l'authenticité et de l'intégrité. Il peut s'agir notamment d'une signature électronique.

Art. 5 Révocation

Le projet de loi prévoit que les émetteurs ont le droit de révoquer des moyens de preuves électroniques en utilisant le registre de base, mais ils n'en ont pas l'obligation. Ils peuvent décider eux-mêmes quand ceux-ci doivent être révoqués et le prévoir dans un contrat avec le titulaire du moyen de preuve électronique. En outre, les tiers, soit des autorités ou des personnes privées, n'ont pas la compétence de révoquer des moyens de preuves électroniques émis par d'autres acteurs.

L'art. 5 n'établit pas d'exigences minimales communes concernant la révocation car les types et les cas d'utilisation de moyens de preuves électroniques sont très variés et régis par des lois différentes. L'article vise uniquement à clarifier le fait que les moyens de preuves électroniques peuvent être révoqués par les émetteurs. Un moyen de preuve électronique révoqué ne peut plus être réactivé: l'émetteur peut toutefois

émettre en tout temps un nouveau moyen de preuve électronique avec le même contenu ou avec un contenu modifié. Les émetteurs peuvent vouloir émettre des moyens de preuves électroniques non révocables lorsqu'une révocation n'est pas utile ou requise et que la procédure de vérification de l'identité est lourde et compliquée.

Bien que le projet de loi ne prévoie pas d'obligation de révocation pour les émetteurs, ceux-ci sont tenus selon l'art. 6, al. 5, LPD de prendre toute mesure appropriée permettant de rectifier, d'effacer ou de détruire les données inexactes ou incomplètes au regard des finalités pour lesquelles elles sont collectées ou traitées. Il est dès lors possible qu'en vertu de cette obligation légale, les émetteurs se voient obligés, dans certains cas, de révoquer des moyens de preuves électroniques ou de trouver d'autres mesures techniques à mettre en œuvre pour assurer le respect de la LPD.

Art. 6 Forme et conservation des moyens de preuves électroniques

Le titulaire reçoit une preuve électronique sous la forme d'un paquet de données. Ce paquet de données est stocké sur le support technique du choix du titulaire. Le projet de loi ne contient pas d'exigences par rapport aux moyens techniques qui doivent être utilisés pour conserver un moyen de preuve électronique. En revanche, la Confédération met à disposition une telle application, qui est strictement conçue selon les principes de la protection des données par la technique et les préréglages par défaut (cf. commentaire de l'art. 7).

Art. 7 Application pour la conservation et la présentation des moyens de preuves électroniques

Al. 1

L'OFIT met à disposition une application pour la conservation et la présentation des moyens de preuves électroniques, dite portefeuille électronique étatique. Il s'agit d'une application logicielle qui permet de demander, d'obtenir de manière sécurisée, de stocker, de sélectionner, de combiner et de partager des moyens de preuves électroniques d'une manière transparente et traçable pour l'utilisateur. L'e-ID et d'autres moyens de preuves électroniques peuvent en faire partie. Dans la mesure où cela est requis, la mise en place du portefeuille électronique étatique tient compte des normes élaborées par l'UE.

La loi ne règle pas l'utilisation des portefeuilles électroniques émis par d'autres acteurs. En sus du portefeuille électronique étatique, les utilisateurs peuvent se servir d'autres applications pour la conservation et la présentation de leurs moyens de preuves électroniques.

Al. 2

Après une perte ou 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. La même possibilité pourra être offerte aux titulaires du portefeuille électronique étatique.

En tant que fonctionnalité de base de cette application, il est prévu qu'une copie de sauvegarde des moyens de preuves électroniques puisse être créée sur un support de données local du détenteur.

Le présent alinéa délègue au Conseil fédéral la compétence de prévoir que l'OFIT met en place un système informatique dans lequel les titulaires pourront sauvegarder des copies de leurs moyens de preuves électroniques. Après un changement de support technique (smartphone, ordinateur, etc.), ils pourront récupérer rapidement les moyens de preuves électroniques sauvegardés.

L'utilisation du système de copies de sécurité sera volontaire et uniquement possible pour les utilisateurs de l'application visée au présent article. Chaque titulaire sera libre d'utiliser l'option de sauvegarde de ses moyens de preuves électroniques.

Seuls les titulaires auront accès à leurs copies de sécurité. L'OFIT est tenu de concevoir le système de manière à ce que des tiers ne puissent y accéder.

Al. 3

Le présent alinéa délègue au Conseil fédéral la compétence de régler les cas d'inactivité prolongée dans le système de conservation, notamment lorsque des copies de sécurité ne sont pas mises à jour ou ne sont pas utilisées par les titulaires pendant une longue période. Il s'agit d'une mesure permettant de détruire des données pour réduire leur volume accumulé au fil du temps. Avec une mise en œuvre conforme aux exigences de la protection et de la minimisation des données, il ne sera pas possible de connaître le titulaire et donc de le consulter avant une éventuelle destruction de données. Des délais entre deux et cinq ans seront prévus par voie d'ordonnance.

Art. 8 Application pour la vérification des moyens de preuves électroniques

Al. 1

L'OFIT met à disposition une application permettant de vérifier la validité de l'e-ID. Il s'agit d'une mesure de sécurité qui vise à faciliter la vérification de l'e-ID et à garantir que cette vérification est sûre. En outre, elle permet d'augmenter la confiance dont bénéficie l'infrastructure prévue par la loi. L'utilisation de l'application est volontaire: chaque vérificateur est libre d'y recourir pour vérifier l'e-ID émise par fedpol.

Al. 2

Le Conseil fédéral pourra décider de permettre la vérification de la validité des autres moyens de preuves électroniques avec l'application prévue. Cette option pourrait être une mesure importante pour faciliter l'usage de l'infrastructure de confiance et des moyens de preuves numériques. Il sera également facultatif d'utiliser cette application pour vérifier la validité des autres moyens de preuves électroniques. Chaque vérificateur sera libre de décider s'il veut recourir à l'application de la Confédération ou à une autre application équivalente disponible sur le marché.

Art. 9 Présentation des moyens de preuves électroniques

Al. 1

Le titulaire n'est pas obligé de présenter ses moyens de preuves électroniques dans leur intégralité. Il est libre de décider quelles parties d'un moyen de preuve électronique ou quelles informations découlant de ce dernier il présentera au vérificateur, dans un cas concret, pour que le but de la vérification soit rempli. La conception des moyens de preuve électroniques sera définie par voie d'ordonnance afin d'assurer que les émetteurs prévoient la possibilité de transmettre certains ou tous les éléments d'un moyen de preuve électronique.

Le projet de loi ne contient pas d'exigences par rapport aux types de données qui doivent être communiquées lors de la vérification des moyens de preuves électroniques. Sur le plan de la réalisation technique, il faudra que les parties d'un moyen de preuve électronique puissent être présentées individuellement pendant que la vérification de l'authenticité et de l'intégrité reste entièrement possible.

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 par le vérificateur, il ne pourra potentiellement pas accéder au service offert par celui-ci.

La LPD pose toutefois des limites par rapport aux données que les vérificateurs peuvent exiger d'un titulaire d'un moyen de preuve électronique. L'art. 6, al. 2, LPD prévoit notamment que le traitement des données personnelles doit être conforme aux principes de la bonne foi et de la proportionnalité. En outre, les données personnelles ne peuvent être collectées que pour les finalités déterminées et reconnaissables pour la personne concernée et doivent être traitées ultérieurement de manière compatible avec ces finalités (art. 6, al. 3, LPD).

Al. 2

L'infrastructure de confiance est conçue par l'OFIT de manière à ce que l'émetteur d'un moyen de preuve électronique n'ait pas connaissance des informations liées à la présentation et à la vérification de ce dernier.

Al. 3

Le registre de base et le registre de confiance ne permettent pas à l'OFIT d'accéder au contenu des moyens de preuves électroniques présentés, car ces données ne sont pas stockées dans ces registres. En outre, il lui est impossible de tirer des conclusions sur l'utilisation d'un moyen de preuve électronique et sur les autorités et les personnes privées concernées. En tant qu'exploitant de l'infrastructure de confiance, il peut toutefois accéder aux données personnelles générées lors de la consultation du registre de base visé à l'art. 2 et du registre de confiance visé à l'art. 3, par exemple aux adresses IP ou autres informations similaires selon le protocole utilisé.

Art. 10 Signalement de cyberattaques contre les émetteurs et les vérificateurs

La consultation a également révélé qu'il y a lieu de prévoir une obligation de signaler les cyberattaques contre les systèmes d'émission et de vérification. Ne bénéficiant pas des droits d'accès requis, l'OFIT n'est pas en mesure de détecter les cyberattaques contre des systèmes recourant à l'infrastructure de confiance. Donc, l'obligation de signaler est essentielle pour assurer une protection efficace des utilisateurs de l'infrastructure de confiance de la Confédération.

Toutefois, il y a lieu de coordonner l'art. 10 avec la modification de la loi du 18 décembre 2020 sur la sécurité de l'information (LSI)[25], qui est en cours d'examen au Parlement[26]. L'art 74*b* prévoit une nouvelle obligation de signalement des cyberattaques contre les infrastructures critiques. Au cas où cette modification serait acceptée par le Parlement et entrerait en vigueur, le présent projet prévoit la disposition de coordination suivante:

Art. 74b, let. v

[1] L'obligation de signaler s'applique:

v. aux émetteurs et aux vérificateurs de moyens de preuves électroniques au sens de la loi du ... sur l'e-ID.

Art. 11 Code source de l'infrastructure de confiance

Al. 1

La Confédération publie sur Internet le code source des composants de l'infrastructure de confiance visés aux let. a à d. Cette mesure permet d'augmenter la confiance dont bénéficie cette infrastructure auprès de la population et de maintenir un niveau de sécurité élevé en permettant aux personnes intéressées de tester le code publié. En outre, cet alinéa vise à maintenir l'esprit d'ouverture qui fait partie de l'approche participative du projet.

Al. 2

L'OFIT peut décider exceptionnellement de ne pas publier le code source ou une partie de celui-ci s'il existe des raisons de croire que la sécurité informatique d'un des composants visés à l'al. 1, let. a à d, pourrait être compromise par une telle publication. À titre d'exemple, il serait envisageable de ne pas publier le code source de composants du processus de vérification de l'identité en ligne, dans la mesure où ce processus est mis en œuvre au moyen de l'application visée à l'art. 7 (porte-monnaie électronique étatique).

25 RS **128**

26 Message du 2 décembre 2022 relatif à la modification de la loi fédérale sur la sécurité de l'information au sein de la Confédération (Mise en place d'une obligation de signaler les cyberattaques contre les infrastructures critiques), FF **2023** 84 85; www.parlement.ch > Travail parlementaire > Recherche Curia Vista > 22.073.

Le projet de loi ne règle pas expressément les mesures techniques et organisationnelles qui doivent être prises dans le cadre de l'infrastructure de confiance. Afin d'éviter des répétitions et de faciliter la compréhension, le projet de loi ne renvoie pas à l'art. 8 LPD, aux art. 3 et 4 de l'ordonnance du 31 août 2022 sur la protection des données (OPDo)[27] ni aux dispositions de la LSI en ce qui concerne les mesures techniques et organisationnelles appropriées que l'OFIT doit prendre pour assurer une sécurité élevée et proportionnée aux risques encourus dans le cadre de l'exploitation de l'infrastructure de confiance. Il ne prévoit pas non plus expressément que l'OFIT est tenu d'effectuer des contrôles réguliers des éléments clés de l'infrastructure de confiance en se fondant sur les normes nationales et internationales reconnues en la matière. Il s'agit d'une mesure technique qui est typiquement prise en pratique afin d'assurer une sécurité élevée de l'infrastructure informatique exploitée; elle ne requiert pas de base légale au sens formel.

Section 3 E-ID

Art. 12 Forme

L'OFIT met en place une infrastructure de confiance (cf. section 1) qui permet à des acteurs publics et privés (cf. limitation de l'art. 3, al. 4) d'émettre divers moyens de preuves sous forme électronique, moyens qui peuvent être utilisés en tant que justification de l'identité, d'un fait ou d'un événement (moyens de preuves électroniques). L'e-ID est un moyen de preuve électronique qui atteste l'identité du titulaire et qui est émis exclusivement par fedpol au travers de l'infrastructure de confiance étatique. En particulier, l'e-ID est une «pièce justificative» au sens de l'art. 3 de la loi du 10 octobre 1997 sur le blanchiment d'argent[28].

Art. 13 Conditions personnelles

Remarque préliminaire

Pour qu'une personne puisse demander une e-ID, elle doit déjà disposer d'un document d'identité délivré par une autorité suisse. Cette condition a l'avantage de garantir que cette personne a été identifiée par une autorité suisse et que des données actuelles la concernant sont disponibles.

Les personnes 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 à l'intention du requérant. Le requérant devient un titulaire lorsqu'il obtient l'e-ID.

Let. a

Ch. 1

Pour demander l'émission d'une e-ID, il suffit au citoyen suisse d'avoir un document d'identité valable au sens de la LDI. Cette réglementation inclut les Suisses de l'étranger. Les personnes morales, agissant toujours par l'intermédiaire de leur organe, au-

27 RS **235.11**
28 RS **955.0**

trement dit des personnes physiques, ne peuvent pas être titulaires d'une e-ID et sont identifiées au moyen du numéro d'identification unique des entreprises (IDE)[29].

Ch. 2

Tous les étrangers qui possèdent une autorisation valable au sens de la LEI et de l'ordonnance du 24 octobre 2007 relative à l'admission, au séjour et à l'exercice d'une activité lucrative (OASA)[30] pourront obtenir une e-ID. Il s'agit des permis suivants:

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

Il est indéniable qu'avec cette réglementation, tous les étrangers qui sont en contact avec les autorités suisses ne sont pas autorisés à demander une e-ID (par ex. les étrangers qui possèdent une maison de vacances en Suisse). En raison du fait que ces personnes n'ont jamais été formellement identifiées par une autorité suisse, aucune e-ID ne peut leur être délivrée. Cette réglementation n'exclut pas que les autorités qui sont en contact étroit avec ces personnes leur délivrent une autre preuve électronique d'identification.

Les e-ID émises pour les citoyens suisses et pour les étrangers sont équivalentes. Toutefois, 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 projet de loi n'introduit pas de limitations d'accès aux services en ligne et laisse une marge de manœuvre aux prestataires de services concernés. Lorsque cela est justifié et permis par la législation applicable, 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.

29 www.bfs.admin.ch > Registres > Registres des entreprises > Numéro d'identification des entreprises IDE
30 RS **142.201**

Pour certaines catégories de permis (par 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 requérants 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 (Secrétariat d'État aux migrations) 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.

Ch. 3

Tous les étrangers qui possèdent une carte de légitimation valable au sens de l'art. 17, al. 1, de l'ordonnance du 7 décembre 2007 sur l'État hôte (OLEH)[31] en relation avec l'art. 71*a*, al. 1, OASA peuvent obtenir une e-ID.

Let. b

La let. b prévoit la possibilité d'émettre une e-ID pour une personne intéressée après l'expiration de la durée de validité de son document d'identité ou d'une pièce de légitimation ou carte de légitimation. L'e-ID pourra être à émise à deux conditions: (1) la demande d'établissement d'un document d'identité au sens de la LDI ou d'une pièce de légitimation valable au sens de la législation fédérale sur les étrangers, l'intégration et l'asile a été soumise en personne et (2) la demande de l'e-ID a été soumise en personne. Les deux demandes peuvent être présentées dans le cadre d'un même rendez-vous auprès de l'autorité compétente. Avant d'émettre l'e-ID, l'autorité compétente doit vérifier l'identité du requérant. La possibilité prévue à la let. b répond aux besoins de la pratique et vise à assurer une expérience utilisateur conviviale lors de l'émission de l'e-ID.

Art. 14 Contenu

Al. 1

L'e-ID contient les données d'identification personnelles suivantes:

a. le nom officiel;

b. les prénoms;

c. la date de naissance;

d. le sexe;

e. le lieu d'origine; il s'agit d'une particularité suisse, qui a été conservée pour être incluse dans l'e-ID et faciliter ainsi certaines démarches administratives en Suisse;

f. le lieu de naissance; le lieu de naissance est souvent requis dans le cadre des transactions internationales et a été inclus pour cette raison dans l'e-ID;

31 RS **192.121**

g. la nationalité; comme les étrangers disposant d'un permis de séjour suisse peuvent également obtenir une e-ID, il convient de mentionner la nationalité dans leur e-ID; cette information est souvent requise dans le cadre de transactions nationales et internationales;

h. la photographie;

i. le numéro AVS; le numéro AVS, en tant que numéro univoque et persistant tout au long de la vie, est très utile pour les démarches administratives; il ne peut être consulté que par les autorités autorisées par la loi.

Ces données sont disponibles dans les registres officiels de l'État auxquels fedpol a accès conformément à l'art. 25, al. 3, et sont reprises dans l'e-ID sans modification.

Al. 2

En sus des données d'identification personnelles de base, une e-ID contient des informations supplémentaires. Il s'agit des données suivantes: le numéro de l'e-ID, sa date d'émission, sa date d'expiration, les indications relatives au document d'identité qui a été utilisé lors de son émission, notamment son type et sa date d'expiration et des indications relatives à la procédure d'émission.

Al. 3

Cet alinéa a été introduit afin de tenir compte des résultats de la consultation. Certains participants ont souligné que les documents d'identité des titulaires de l'e-ID peuvent également contenir des données supplémentaires, telles que le nom du représentant légal, le nom d'alliance, le nom reçu dans un ordre religieux, le nom d'artiste ou le nom de partenariat et la mention de signes particuliers. Ces données peuvent être utiles, voire nécessaires, dans le cadre de certaines transactions que les titulaires de l'e-ID réaliseront. Elles peuvent être contenues dans l'e-ID à condition qu'elles soient également indiquées dans le document d'identité, la pièce de légitimation ou la carte de légitimation du titulaire.

Art. 15 Demande

Al. 1

Il n'y a pas d'obligation d'obtenir une e-ID. Si quelqu'un veut en obtenir une, il doit la requérir auprès de fedpol. La demande doit émaner du futur titulaire de l'e-ID (requérant) et le cas échéant être autorisée par son représentant légal (voir al. 3, 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 via le système d'information de fedpol ou le portefeuille électronique étatique visé à l'art. 7.

Al. 2

Afin de tenir compte des résultats de la consultation, l'al. 2 prévoit la possibilité d'émettre simultanément plusieurs e-ID. La consultation externe a révélé qu'un tel besoin existe en pratique. Par exemple, un parent pourrait avoir besoin de l'e-ID de son enfant pour réaliser des transactions en son nom. Pour certaines personnes, il pourrait être utile d'enregistrer leur e-ID sur plusieurs supports techniques, tels un smart-

phone privé, un smartphone professionnel et une tablette ou un ordinateur portable. Afin de prévenir des abus éventuels, il est prévu toutefois qu'une telle émission doit avoir lieu simultanément. Une fois l'e-ID ou les e-ID émises, un titulaire ne pourra plus faire de demande d'émission d'une e-ID additionnelle sur un autre support (sans que l'e-ID existante ne soit révoquée [art. 18, let. e]). Dans ce cas, il devra soumettre une nouvelle demande pour tous ses supports et les anciennes e-ID seront révoquées.

Al. 3

Selon cet alinéa, les mineurs ainsi que les personnes sous curatelle de portée générale requièrent l'autorisation de leur représentant légal pour l'obtention de l'e-ID. Cette exigence s'aligne sur la limite d'âge prévue pour l'obtention des documents d'identité suisses (soit 18 ans; art. 5, al. 1, LDI). Le représentant légal d'un mineur ou d'une personne sous curatelle de portée générale peut conserver l'e-ID de ce dernier ou de cette dernière et sa propre e-ID dans le portefeuille électronique visé à l'art. 7.

Art. 16 Vérification de l'identité

Al. 1

Cet alinéa a été introduit afin de tenir compte des résultats de la consultation. De nombreux participants à la consultation ont estimé que le projet de loi devrait prévoir la possibilité d'obtenir l'e-ID en se présentant en personne. Ainsi, cet alinéa permet au requérant de faire vérifier son identité en ligne auprès de fedpol ou en personne auprès de services ou d'autorités compétentes désignés par les cantons en Suisse et par le Conseil fédéral à l'étranger. Des consultations ont été entamées avec les cantons afin d'évaluer la possibilité de mettre en place des procédures de vérification de l'identité au sein des bureaux des passeports et des offices des migrations cantonaux, entre autres.

Al. 2

Le présent alinéa donne la compétence aux services et aux autorités visés à l'al. 1 de vérifier au travers d'une comparaison si le visage du requérant de l'e-ID correspond à la photographie contenue dans les registres fédéraux ISA, SYMIC ou Ordipro. Cette vérification peut avoir lieu en personne ou en ligne. Les modalités de cette procédure seront définies par le Conseil fédéral au niveau de l'ordonnance (art. 19, let. b).

Al. 3

Cet alinéa constitue une base légale au sens formel permettant à fedpol de collecter des données biométriques pour effectuer la comparaison visée à l'al. 2. Celle-ci sera effectuée lors du processus en ligne. L'al. 3 satisfait ainsi aux exigences de l'art. 34, al. 2, let. a, LPD, en vertu duquel, une base légale dans une loi au sens formel est requise pour permettre aux organes fédéraux de traiter des données sensibles. L'art. 5, let. c, ch. 4, LPD dispose que «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 comporte-

mentales d'une personne physique qui permettent ou confirment son identification unique»[32].

Dans le cadre de la consultation, certains participants ont demandé que les données biométriques recueillies pendant le processus d'émission de l'e-ID soient immédiatement détruites. Le projet de loi ne prévoit pas de telle obligation, car il vise à permettre à fedpol de conserver ces données biométriques, qui sont nécessaires en cas d'enquête concernant l'obtention frauduleuse d'une e-ID (art. 26, al. 1, let. b). Par conséquent, ces données peuvent être conservées jusqu'à cinq ans après la fin de la validité de l'e-ID.

Art. 17 Émission

fedpol s'assure que le requérant remplit les conditions définies à l'art. 13. 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 visés à l'art. 25, 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. 14.

Dans la plupart de cas, le processus de vérification de l'identité en ligne se déroulera de manière automatisée. En cas d'incertitude, fedpol peut intervenir et revoir les données générées lors du processus de vérification. Le requérant peut également poser une réclamation auprès du service d'assistance de fedpol. Les exigences de l'art. 21, al. 2, LPD doivent être respectées dans le cadre de ce processus automatisé.

Art. 18 Révocation

Il convient de distinguer la destruction de la révocation de l'e-ID.

La destruction de l'e-ID est un processus irréversible dans lequel le paquet de données composé d'attributs et du matériel cryptographique est supprimé. Du point de vue technique, l'émetteur ne peut pas détruire une e-ID en raison du caractère décentralisé de l'infrastructure de confiance. Seul le titulaire peut supprimer son e-ID en l'effaçant dans son portefeuille électronique ou en désinstallant le portefeuille électronique de son smartphone.

En cas de révocation, une inscription est faite par fedpol au registre de base pour indiquer qu'une e-ID spécifique n'est plus valide. L'e-ID correspondante reste inchangée dans le portefeuille électronique et peut continuer à être présentée. Toutefois, dès qu'un vérificateur procède à une vérification de l'e-ID révoquée, il apprend, à l'aide de l'inscription dans le registre de base, qu'elle n'est plus valide.

Le projet de loi prévoit la possibilité de révoquer une e-ID dans les cas visés aux let. a à e. Le titulaire (adulte, mineur ou personne sous curatelle de portée générale) et le représentant légal d'un mineur 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.

32 Message du 15 septembre 2017 concernant la loi fédérale sur la révision totale de la loi fédérale sur la protection des données et sur la modification d'autres lois fédérales, FF **2017** 6565, en particulier 6640.

En outre, fedpol révoque l'e-ID s'il existe un soupçon fondé qu'elle est utilisée de manière abusive. Avant de procéder à une révocation, fedpol vérifie les informations qui lui ont été soumises. Il révoque également l'e-ID s'il prend connaissance du décès de son titulaire ou du retrait du document d'identité utilisé lors de l'émission de l'e-ID. Ces informations concernant un cas d'abus allégué parviennent à fedpol sous forme de notifications *push* des registres visés à l'art. 25, al. 3. Le Conseil fédéral règle par voie d'ordonnance les devoirs des autorités compétentes concernant l'envoi des notifications requises.

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 toutefois faire une nouvelle demande d'émission au sens de l'art. 15, al. 1, auprès de fedpol.

La révocation est une mesure technique qui ne peut pas être annulée. En outre, elle ne peut pas être communiquée au titulaire de l'e-ID, car il n'est pas certain que le canal de communication avec fedpol qui a été établi lors de la transmission de l'e-ID existe encore. Le titulaire est libre de le supprimer une fois l'e-ID reçue. Le projet de loi prévoit la révocation comme une mesure technique pour prévenir les abus éventuels. Il s'agit d'un compromis entre l'utilisation conviviale de l'e-ID et la nécessité d'assurer un niveau de sécurité élevé. Par ailleurs, la révocation n'entraîne pas le retrait du droit d'obtenir une e-ID. Le titulaire peut refaire une nouvelle demande d'émission.

La révocation de l'e-ID par fedpol constitue un acte matériel et ne donne pas lieu à une décision de la part de fedpol. Le titulaire peut en prendre connaissance lors de l'utilisation de l'e-ID ou de son portefeuille électronique. En outre, il peut contacter l'assistance technique de fedpol pour s'assurer que son e-ID a été révoquée. Il peut également requérir que fedpol statue par décision selon l'art. 25*a* de la loi du 20 décembre 1968 sur la procédure administrative[33]. Il devra alors lui fournir les données personnelles supplémentaires qui seront requises pour l'envoi de la décision.

Art. 19 Procédures

Le Conseil fédéral se voit déléguer la compétence de régler les procédures relatives au dépôt de la demande d'émission de l'e-ID (art. 15), à la vérification de l'identité du requérant (art. 16), à l'émission (art. 17) et à la révocation (art. 18) de l'e-ID.

Art. 20 Durée de validité

Pour des raisons de sécurité, l'e-ID a une durée de validité limitée. 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. 14, al. 2, let. b et c). Si ce document d'identité utilisé lors de l'émission de l'e-ID est retiré par les autorités, l'e-ID sera révoquée par fedpol au moment où il prend connaissance du retrait (art. 18, let. d, ch. 1).

Une e-ID qui n'est plus valide reste disponible sur le support électronique du titulaire en tant que moyen de preuve électronique authentique mais échu.

33 RS **172.021**

Art. 21 Devoirs de diligence du titulaire

Al. 1

Les obligations des titulaires d'une e-ID établie dans le cadre du projet de loi correspondent à peu près aux devoirs de diligence qui doivent habituellement être respectés lors de l'utilisation des services bancaires en ligne. 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 cet appareil. 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 pourront être appliquées. Lors de la révision de la LPD, le code pénal[34] a été complété 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, le projet de loi ne contient pas de dispositions sanctionnant le même comportement.

Al. 2

En cas de perte d'un document d'identité physique, la police doit être immédiatement informée (art. 8 LDI). Une réglementation analogue n'a pas de sens pour l'e-ID. Une e-ID devrait toujours bénéficier d'une double protection (sécurisation de l'accès à l'appareil et sécurisation de l'accès au portefeuille électronique). En d'autres termes, un appareil qui tombe entre les mains de personnes non autorisées ne devrait pas permettre d'accéder à l'e-ID qu'il contient. Toutefois, le titulaire peut à tout moment – donc également en cas de perte – demander la révocation de l'e-ID (art. 18, let. a).

Si le titulaire soupçonne une utilisation abusive de son e-ID, il doit le signaler immédiatement à fedpol et, le cas échéant, demander la révocation de son e-ID.

Art. 22 Devoir de diligence du vérificateur

Le présent article a été introduit pour tenir compte des résultats de la consultation. L'absence de disposition restreignant le traitement des données par les vérificateurs a fait l'objet de nombreuses critiques et propositions. La principale critique concernait le fait que les vérificateurs peuvent décider librement de l'exigence de présenter un moyen de preuve électronique et de son étendue, alors que selon certains participants celle-ci devait être limitée par la loi au strict nécessaire et assujettie à un consentement éclairé et explicite. Par ailleurs, selon eux, l'avant-projet de loi et la LPD ne protègaient pas suffisamment les titulaires des moyens de preuves électroniques contre le risque de recours injustifié à l'identification électronique par les vérificateurs.

Lors de l'élaboration de la présente disposition, il a été constaté que des sanctions efficaces peuvent uniquement être imposées dans le cadre de l'utilisation de l'e-ID. Les cas d'utilisation des autres moyens de preuve électroniques sont trop diversifiés et pas assez connus pour permettre d'imposer des sanctions uniformes. Ensuite, il est

34 RS **311.0**

apparu que des sanctions pénales n'étaient pas le meilleur outil pour prévenir des violations de l'al. 1. Au vu des sanctions pénales qui sont prévues pour la violation des diverses dispositions de la LPD, une violation de l'al. 1 ne semble pas revêtir la même gravité et ne pourrait pas être punie par voie d'une sanction comparable. En outre, les exigences de l'al. 1 laissent une marge d'interprétation importante et ne sont pas bien adaptées à l'imposition d'une sanction pénale. Les sanctions pénales évaluées donnent lieu à des incohérences et des inégalités importantes en pratique. Des exigences plus précises, telles l'inscription obligatoire au registre de confiance des vérificateurs recourant à l'e-ID, pourraient être sanctionnées en cas de non-respect mais sont diamétralement opposées aux principes fondamentaux de la SSI et impose un fardeau bureaucratique important. Enfin, il s'est avéré que la communication des violations aux autres utilisateurs et l'exclusion du vérificateur fautif constituent des sanctions plus utiles et plus efficaces du comportement reproché.

La possibilité de régler d'autres aspects, telle une obligation étendue d'informer le titulaire, un droit étendu du titulaire de s'opposer ou l'interdiction de couplage[35] (instruments visant à lutter contre la «suridentification»), a été examinée pour donner suite aux critiques et arguments formulés par les participants à la consultation. Au vu des difficultés techniques dans la mise en œuvre de telles exigences, il n'a pas été possible de définir de nouvelles règles communes en la matière. En outre, le Conseil fédéral ne souhaite pas relancer la discussion concernant les compromis convenus en matière de sanctions dans le cadre de la LPD.

Les dispositions de la LPD et le code civil (CC)[36] restent applicables en la matière. Il convient de rappeler que le traitement des données personnelles contenues dans l'e-ID doit être proportionnel (adéquat, pertinent et non excessif) aux finalités déterminées par le vérificateur (art. 6, al. 2 LPD).

Al. 1

Pour donner suite aux préoccupations exprimées lors de la consultation, l'al. 1 vise à renforcer les exigences de la LPD et de l'avant-projet en ce qui concerne l'utilisation de l'e-ID. Il fixe les conditions auxquelles le vérificateur peut demander aux titulaires de transmettre des données personnelles contenues dans l'e-ID: ce dernier peut requérir la transmission de ces données uniquement lorsque la vérification de l'identité ou d'un aspect de l'identité du titulaire est prévue par la loi (let. a) ou est nécessaire pour des raisons de fiabilité de la transaction (let. b). Le présent alinéa vise ainsi à limiter la possibilité de demander des données personnelles qui ne sont pas essentielles à la fourniture d'une prestation. Il s'agit de prévenir les cas de recours injustifié à l'identification électronique par les vérificateurs.

Let. a

Un exemple de transfert de données personnelles pour la finalité prévue à la let. a serait une demande d'accès au sens des 25 LPD et 16, al. 3, OPDo. La personne qui

35 Au sens de l'art. 7, par. 4, du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE, JO L 119 du 4.5.2016, p. 1.

36 RS **210**

demande au responsable du traitement d'accéder aux informations pertinentes reçoit notamment des informations sur son identité. Il pourrait également s'agir de l'obligation prévue à l'art. 20 de l'ordonnance du 15 novembre 2017 sur la surveillance de la correspondance par poste et télécommunication (OSCPT)[37]; selon laquelle les fournisseurs de service de télécommunication (FST) et des revendeurs de vérifier l'identité de l'usager. En outre, l'art. 17 de l'ordonnance du 11 novembre 2015 sur le blanchiment d'argent (OBA)[38], qui prévoit une obligation de vérification de l'identité d'un cocontractant par le négociant lors de la conclusion d'un contrat, remplit également les exigences de la présente lettre. De plus, l'obligation de s'identifier dans le cadre de la demande d'un dossier électronique du patient constituera également un cas d'application de la présente lettre suite à la modification de la législation relative au dossier électronique du patient.

Let. b

Dans le cadre d'une transmission de données personnelles pour la finalité prévue à la let. b, il pourrait s'agir d'une vérification de l'identité d'une personne pour passer un examen organisé par une université ou une autre institution de formation. En outre, il pourrait être également nécessaire de vérifier l'identité d'une personne lors de la livraison d'un colis par le service de livraison. La vérification de l'identité constitue dans ces cas un élément essentiel.

Toutefois, la vérification de l'identité d'un consommateur dans le cadre d'une commande sur facture qu'il passe sur Internet ne remplit pas les exigences de la let. b. Le vendeur pourrait vouloir s'assurer au moyen de l'e-ID que son interlocuteur est majeur et qu'il existe bien. Il s'agit d'un besoin réel et important, mais pas d'une nécessité liée à la fiabilité de la transaction, qui requerrait que le vendeur vérifie notamment la solvabilité ou l'adresse pour s'assurer que la personne qui commande sans payer est solvable et recevra sa commande. La vérification de l'identité au moyen de l'e-ID ne permet d'obtenir ni l'adresse ni des informations sur la solvabilité de la personne concernée. La demande des données personnelles contenues dans l'e-ID n'augmente pas automatiquement le niveau de fiabilité d'une commande sur facture.

Al. 2

En vertu de l'al. 2, l'OFIT publie dans le registre de confiance une liste de cas d'identification au moyen de l'e-ID qui violent les exigences de l'al. 1. Il s'agit d'une mesure de sécurité essentielle servant à prévenir les violations futures et à informer les utilisateurs sur les violations connues. N'ayant pas la compétence de détecter ces violations, l'OFIT agit lorsqu'il prend connaissance d'un tel cas. Il vérifie la crédibilité des informations avant de les publier. Lorsqu'un vérificateur est inscrit au registre de confiance et ne respecte pas les exigences de l'al. 1, l'OFIT peut en outre décider de l'exclure du registre de confiance.

37 RS **780.11**
38 RS **955.01**

Art. 23 Obligation d'accepter l'e-ID

Les autorités et les autres organismes accomplissant des tâches publiques doivent accepter l'e-ID lorsqu'ils recourent à l'identification électronique en exécution du droit fédéral. Les autorités des cantons et des communes sont incluses parmi les destinataires de cette norme. En font par exemple partie les offices des poursuites auprès desquels un particulier demande un extrait du registre par la voie électronique et s'identifie avec une e-ID (cf. le commentaire de l'art. 33*a,* al. 2bis, LP). Cela est indiqué parce que l'e-ID est conçue en tant que moyen d'identification électronique étatique servant à 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. L'e-ID étatique pourra être utilisée conjointement avec les moyens d'accès aux services cyberadministratifs existants. Cette obligation ne s'applique qu'aux processus d'identification nécessitant la présence du titulaire et la présentation d'une pièce d'identité.

L'art. 23 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 2018–2022[39] et la Stratégie suisse de cyberadministration 2020–2023[40]. 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 et les conséquences juridiques s'y rapportant ne sont pas réglées dans le projet de loi. Elles doivent être réglées de manière spécifique pour chaque secteur. Le projet de loi tient notamment compte du dossier électronique du patient ainsi que des poursuites pour dettes et de la faillite.

Art. 24 Alternative à la présentation d'une e-ID

Cet 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'un 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. 25 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. 14. Le système d'information permettra de recevoir les demandes des

39 www.uvek.admin.ch > Communication > Stratégie Suisse numérique
40 www.bk.admin.ch > Transformation numérique et gouvernance de l'informatique > Directives informatiques > Stratégies et stratégies partielles > SN001 – Stratégie suisse de cyberadministration

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 visées à l'art. 14, al. 2, concernant les e-ID demandées et émises ainsi que les données liées à la révocation d'une e-ID. En outre, on y conserve également les données relatives à la procédure d'émission, qui sont requises à des fins d'assistance technique et de statistique ou d'enquête concernant l'obtention frauduleuse ou l'utilisation abusive d'une e-ID.

Al. 3

Le système d'information pourra accéder aux données visées à l'art. 14, al. 1, et contenues dans les registres de personnes suivants, gérés au niveau fédéral, afin d'émettre l'e-ID:

- le système d'information relatif aux documents d'identité (ISA) visé à l'art. 11 LDI;
- le système d'information central sur la migration (SYMIC) visé aux art. 101 ss LEtr et dans l'ordonnance SYMIC du 12 avril 2006[41];
- le registre informatisé de l'état civil (Infostar) visé aux art. 39 CC et 6*a* de l'ordonnance du 28 avril 2004 sur l'état civil (OEC)[42];
- le registre central de la centrale de compensation de l'AVS (CdC-UPI) visé à l'art. 71, al. 4, de la loi du 20 décembre 1946 sur l'assurance-vieillesse et survivants (LAVS)[43]; seule la partie UPI du registre, responsable de la gestion du numéro AVS et des données mentionnées à l'art. 133[bis], al. 4, du règlement du 31 octobre 1947 sur l'assurance-vieillesse et les survivants[44], est accessible;
- le système d'information Ordipro du Département fédéral des affaires étrangères visé aux art. 5 de la loi fédérale du 18 décembre 2020 sur le traitement des données personnelles au Département fédéral des affaires étrangères[45] et 2 de l'ordonnance Ordipro du 22 mars 2019[46].

fedpol pourra ainsi exécuter les tâches requises pour l'émission des e-ID d'une manière automatisée. Sur cette base, il pourra vérifier l'identité du requérant.

Al. 4

Les données obtenues via des interfaces ne sont ni dupliquées ni sauvegardées dans le système d'information de fedpol. Elles sont contrôlées directement dans les registres fédéraux. fedpol les traite uniquement dans le but d'émettre et de révoquer l'e-ID. Toute autre finalité de traitement de ces données est ainsi exclue.

41 RS **142.513**
42 RS **211.112.2**
43 RS **831.10**
44 RS **831.101**
45 RS **235.2**
46 RS **235.21**

Art. 26 Conservation et destruction des données

Al. 1

Cet article a été introduit pour tenir compte des résultats de la consultation externe. Certains participants ont regretté que l'avant-projet de loi ne règle pas la durée de conservation et la destruction des données. Conformément à l'art. 6, al. 4, LPD, les données personnelles sont détruites ou anonymisées dès qu'elles ne sont plus nécessaires au regard des finalités du traitement. Ces finalités découlent des bases légales prévues pour le traitement des données aux art. 14 et 25 du présent projet de loi. L'art. 26 prévoit des délais de conservation distincts pour trois catégories de données tenant compte de leurs finalités de traitement différentes.

Let. a

Les données visées à la let. a seront conservées 20 ans au plus, à partir de la date de la demande ou de l'émission de l'e-ID. Malgré les délais de conservation différents prévus pour les données contenues dans ISA, SYMIC et Ordipro, les mêmes délais s'appliquent aux données concernant les ressortissants suisses et les étrangers contenues dans le système d'information de fedpol. Afin de simplifier les processus de conservation des données, cette disposition s'aligne sur les délais de conservation prévus pour les données relatives aux documents d'identité suisses visés à l'art. 37, al. 1, de l'ordonnance du 20 septembre 2002 sur les documents d'identité[47]. Ainsi, un seul délai de conservation est prévu pour les données appartenant aux ressortissants suisses et aux étrangers.

Let. b

Les délais fixés pour la conservation des données relatives à la procédure d'émission qui sont nécessaires à des fins d'enquête concernant l'obtention frauduleuse d'une e-ID, y compris des données biométriques visées à l'art. 16, al. 3, se justifient pour des motifs de preuve. Au-delà de ce délai, il n'est pas certain qu'il soit nécessaire de conserver ces données.

Al. 2

Toutes les autres données sont détruites 90 jours après leur enregistrement dans le système. Cette exigence vise à s'assurer que l'article prévoit un délai de conservation pour toutes les données. Les données qui ne sont pas couvertes par l'al. 1 seront conservées selon l'al. 2.

Al. 3

L'al. 1 s'applique à condition que l'art. 38 LPD et les dispositions de la loi fédérale du 26 juin 1998 sur l'archivage (LAr)[48] soient respectés. L'art. 6 LAr dispose que les données qui ne sont plus utilisées sont proposées aux Archives fédérales. Les données que les Archives fédérales jugent sans valeur archivistique sont détruites.

47 RS **143.11**
48 RS **152.1**

Section 4 Accessibilité aux personnes handicapées

Art. 27

Cet article a été introduit afin de tenir compte des résultats de la consultation externe. De nombreux participants ont regretté que l'avant-projet de loi ne contienne pas de dispositions concernant l'accessibilité aux personnes handicapées et ont formulé un certain nombre de demandes à cet égard. Les al. 1 à 3 visent à clarifier et à renforcer les exigences prévues par la loi du 13 décembre 2002 sur l'égalité pour les handicapés (LHand)[49] et par l'ordonnance du 19 novembre 2003 sur l'égalité pour les handicapés (OHand)[50].

Selon l'art. 14, al. 2, LHand, l'accès aux prestations offertes par les autorités sur Internet ne doit pas être rendu difficile aux handicapés de la vue. En outre, l'art. 10, al. 1, OHand prévoit que «l'information et les prestations de communication ou de transaction proposées sur Internet doivent être accessibles aux personnes handicapées de la parole, de l'ouïe, de la vue ou handicapées moteur».

L'art. 27, al. 1 à 3, s'aligne sur les exigences de l'art. 10, al. 1, OHand tout en spécifiant quels composants de l'infrastructure doivent être rendus accessibles aux personnes handicapées. Les exigences de l'OHand ne s'appliquent pas aux applications visées aux art. 7 et 8, car il ne s'agit pas de prestations proposées sur Internet. Les al. 1 à 3 visent à étendre le champ d'application des exigences de l'OHand et de les élever au niveau de la loi.

Al. 1 à 3

L'al. 1 vise à garantir que l'e-ID peut être obtenue par les personnes handicapées. Il charge fedpol de s'assurer que la procédure d'obtention respecte les normes applicables en matière d'accessibilité aux personnes handicapées.

L'al. 2 prévoit également la mise en œuvre de l'accessibilité aux personnes handicapées en relation avec les applications mises à disposition par la Confédération pour faciliter l'utilisation de l'e-ID et d'autres preuves électroniques, soit l'application pour la conservation et la présentation des moyens de preuve électroniques (art. 7) et l'application pour la vérification des moyens de preuve électroniques (art. 8).

Par ailleurs, les normes d'accessibilité aux personnes handicapées devront être respectées dans le cadre de l'obtention et de l'utilisation d'autres moyens de preuve électroniques (al. 3). Les autorités publiques fédérales et cantonales recourant à l'infrastructure de confiance pour émettre et vérifier des moyens de preuve électroniques sont tenues de respecter les normes d'accessibilité aux personnes handicapées dans le cadre de ces processus.

Al. 4

Le Conseil fédéral se voit déléguer la compétence de régler les mesures que fedpol, l'OFIT et les autorités doivent prendre pour garantir l'accessibilité aux personnes handicapées dans les cas prévus aux al. 1 à 3. Il peut notamment prévoir des mesures de

49 RS **151.3**
50 RS **151.31**

communication spécifiques et rendre obligatoires des normes techniques reconnues dans le domaine. En outre, il peut requérir des contrôles et des mises à jour à intervalles réguliers. Le Conseil fédéral consultera les organisations spécialisées et le Bureau fédéral de l'égalité pour les personnes handicapées lors de l'élaboration des dispositions pertinentes.

Section 5 Assistance technique

Art. 28

Les exigences concernant l'assistance prévues dans l'avant-projet de loi ont été remaniées afin de tenir compte des résultats de la consultation. Certains participants ont critiqué le fait que l'avant-projet chargeait les cantons de mettre à disposition des services d'assistance de proximité. Un nombre important de participants ont estimé qu'une assistance devrait être offerte par l'administration fédérale à tous les utilisateurs de l'infrastructure de confiance. L'art. 28 charge donc la Confédération d'offrir un service d'assistance dans le cadre de l'émission de l'e-ID et de l'utilisation de l'infrastructure de confiance. Il s'agira de mettre à disposition un service d'assistance de première ligne dans les trois langues officielles de la Confédération et en anglais. Les autorités fédérales, cantonales et communales ainsi que les personnes physiques pourront y recourir.

Section 6 Progrès technique

Art. 29

Al. 1

La technique progresse à grands pas et continuera d'évoluer après l'entrée en vigueur de la loi. Afin de s'assurer que celle-ci puisse être mise en œuvre, l'al. 1 délègue au Conseil fédéral la compétence 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 une base légale formelle. Par exemple, conformément à l'art. 34, al. 2, let. a, LPD, 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 le cadre du présent projet de loi, l'ordonnance du Conseil fédéral deviendra caduque dans trois cas de figure: si, dans un délai de deux ans après son entrée en vigueur, le Conseil fédéral n'a pas soumis à l'Assemblée 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 7 Émoluments

Art. 30

Al. 1

Des émoluments seront perçus auprès des émetteurs et des vérificateurs pour l'inscription de données dans le registre de base et dans le registre de confiance.

Le montant des émoluments n'étant pas prévu par la loi, il sera défini par voie d'ordonnance. Il pourra s'élever à quelques dizaines ou centaines de francs.

Al. 2

Selon une pratique bien établie, les autorités fédérales ne demandent pas aux autorités cantonales de verser un émolument pour l'utilisation de leur infrastructure (et réciproquement). Ainsi, l'utilisation de l'infrastructure de confiance est gratuite pour les communes et les cantons.

Al. 3

L'alinéa précise qu'aucun émolument n'est perçu pour l'émission de l'e-ID, pour son utilisation, sa vérification et sa révocation, dans la mesure où ces services sont fournis en ligne.

Il convient de préciser que l'utilisation du portefeuille électronique émis par la Confédération, la lecture du registre de base et la lecture du registre de confiance sont gratuites.

En exonérant en grande partie les utilisateurs du paiement d'émoluments, l'al. 3 vise à encourager l'utilisation et la diffusion de l'e-ID. 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.

Al. 4

Cet alinéa a été élaboré afin de tenir compte des résultats de la consultation. Les cantons ont demandé que le projet de loi prévoie la possibilité de percevoir des émoluments pour les services qui sont fournis sur place. Pour donner suite à cette demande, le Conseil fédéral prévoira par voie d'ordonnance que le service compétent peut percevoir des émoluments pour les prestations fournies sur place.

Al. 5

Le Conseil fédéral règle par voie d'ordonnance la perception des émoluments conformément à l'art. 46*a* LOGA.

Section 8 Traités internationaux

Art. 31

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 électroniques. Pour ce faire, un traité international sera requis. L'art. 31 délègue au Conseil fédéral la compétence de conclure des traités internationaux destinés à faciliter l'utilisation et la reconnaissance de l'e-ID sur le plan international et d'adopter les prescriptions d'exécution nécessaires. Un tel traité permettrait d'assurer 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 9 Dispositions finales

Art. 32 Dispositions d'exécution

Les dispositions d'exécution de la présente loi règlent la mise en œuvre des aspects techniques et organisationnels liés au transfert des moyens de preuves électroniques ainsi que le fonctionnement des composants de l'infrastructure de confiance. Il s'agira notamment de régler le format des moyens de preuves électroniques; les normes et protocoles applicables aux processus de communication des données lors de l'émission et de la présentation des moyens de preuves 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 preuves électroniques et du système des copies de sécurité; les preuves à fournir pour l'inscription dans le système de confirmation des identifiants; les mesures techniques et organisationnelles relatives à la sécurité et à la protection des données, dans le cadre de l'exploitation et de l'utilisation de l'infrastructure de confiance et les interfaces ainsi que les éléments et le fonctionnement du système d'information pour l'émission et la révocation des e-ID.

Art. 33 Modification d'autres actes

Le 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 des poursuites et de la faillite.

Art. 34 Disposition transitoire

Al. 1

Selon l'art. 23, les autorités et les organismes qui accomplissent des tâches publiques doivent accepter l'e-ID lorsqu'ils recourent à l'identification électronique en exécution du droit fédéral. Le présent alinéa prévoit un délai de deux ans à partir de l'entrée en vigueur de la loi pour la mise en œuvre de cette obligation.

Al. 2

Pour garantir la sécurité, la qualité du système et la disponibilité de l'assistance technique lors de son introduction, le Conseil fédéral peut prévoir une mise à disposition échelonnée de l'infrastructure de confiance et de l'e-ID durant au maximum deux ans

suivant l'entrée en vigueur de la présente loi. Il s'agit notamment des différentes fonctionnalités liées au portefeuille électronique comme l'enregistrement d'e-ID multiples sur différents supports ou de l'enregistrement de l'e-ID sur des portefeuilles de prestataires tiers. Le présent alinéa vise à s'assurer de la maturité du produit à chaque étape de la mise en œuvre.

Le Conseil fédéral peut également prendre des mesures permettant de garantir une mise à disposition qualitative et sûre des émissions en ligne. Les expériences d'autres pays ont démontré que les premiers mois sont soumis à une forte demande, ce qui met sous pression l'assistance et l'encadrement technique du système. Pour garantir une introduction du système qualitative et sûre, un monitoring du nombre d'e-ID émises par jour pourrait être mis en œuvre durant les premiers mois, impliquant potentiellement un délai d'attente pour les requérants.

Le Conseil fédéral peut également prévoir un échéancier pour permettre aux autorités compétentes pour la vérification de l'identité en personne (art. 16, al. 1, let. b) de s'organiser et assumer cette nouvelle tâche, comme les cantons l'ont souhaité (cf. ch. 6.2).

Art. 35 Référendum et entrée en vigueur

Comme toute loi fédérale, la loi est sujette au référendum. Le Conseil fédéral fixera la date de son entrée en vigueur.

Modifications d'autres actes

Remarque préliminaire

Les conditions d'identification et d'authentification pour les applications de la cyberadministration sont réglées dans le droit applicable et, dans la mesure où elles sont nécessaires, 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, raison pour laquelle seules les modifications d'autres lois fédérales sont expliquées dans la présente section.

Suite à une évaluation des divers domaines du droit fédéral, il apparaît que seules les lois présentées ci-dessous doivent être modifiées dans le cadre du présent projet. Cette évaluation a tenu compte de tous les domaines pertinents du droit fédéral. En outre, des discussions ont été organisées avec les départements fédéraux intéressés à recourir à l'e-ID. Il existe peu de domaines où le droit fédéral requiert d'identifier la personne concernée. Par ailleurs, la loi ne vise pas à régler tous les domaines où les moyens de preuves électroniques seront utilisés. Elle sert à mettre en place les bases légales requises pour l'utilisation de l'e-ID et de l'infrastructure de confiance. Dans la mesure où cela est nécessaire, il appartiendra aux autorités compétentes de prévoir les bases légales requises dans des lois sectorielles.

1. Loi fédérale du 20 juin 2003 sur le système d'information commun aux domaines des étrangers et de l'asile (LDEA)[51]

Art. 9, al. 1, let. c, ch. 7bis, 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 traitées 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 sûreté intérieure. Il s'agit d'ajouter à cette liste un nouveau but, notamment l'accomplissement des tâches qui leur incombent en vertu de la présente 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 traitées 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 sûreté intérieure. Le projet ajoute un nouveau but à cette liste, notamment l'accomplissement des tâches qui leur incombent en vertu de la loi sur l'e-ID.

2. Loi du 22 juin 2001 sur les documents d'identité

Art. 1, al. 3, 2e phrase

En principe, seules les personnes de nationalité suisse peuvent se voir délivrer un passeport diplomatique ou un passeport de service suisse. Pour des raisons de sécurité, il peut être nécessaire d'en délivrer également à des personnes ne possédant pas la nationalité suisse pour certains États de résidence ou en vue de l'exercice de certaines missions dans l'intérêt et sur mandat de la Suisse. Il s'agit d'éviter que les personnes accompagnantes étrangères de diplomates suisses ou d'autres employés d'une représentation à l'étranger ne s'exposent à de graves inconvénients. Dans certains cas, il est indispensable de posséder un passeport diplomatique ou un passeport de service suisse pour être admis dans l'État accréditaire et, le cas échéant, se faire délivrer un visa. Les évolutions sociétales en matière de partenariats, et notamment le fait que de plus en plus de diplomates ont un conjoint ou un partenaire étranger, a donné une acuité supplémentaire à la problématique mentionnée. Un autre enjeu est de faciliter dans des cas particuliers l'exercice de certaines fonctions par des collaborateurs étrangers. Pour certaines missions dans des zones de crise ou de guerre, qui impliquent des risques accrus pour la vie et l'intégrité corporelle, le DFAE peut devoir faire appel à des spécialistes qui ne possèdent pas la nationalité suisse, mais la personne recrutée n'acquiert pas pour autant la nationalité suisse. Sur la page des données personnelles du passeport, le pays d'origine du titulaire est donc également mentionné dans la rubrique «nationalité», et le lieu d'origine est remplacé par «***».

Art. 11, al. 2, 2e phrase

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

51 RS **142.51**

3. Code civil

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

Art. 33a, al. 2bis

Conformément à l'art. 33*a*, al. 1, LP, les requêtes peuvent être déposées par voie électronique auprès des offices des poursuites et des faillites et des autorités de surveillance. Elles doivent être munies d'une signature électronique qualifiée (art. 33*a*, 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 plateforme de la Confédération. Cela permet de simplifier le processus de saisie pour toutes les personnes concernées.

Le Conseil fédéral déterminera quelles plateformes pourront être utilisées. On songe avant tout aux plateformes de communication électronique dans le domaine judiciaire[52] et à la plateforme EasyGov[53] gérée par le Secrétariat d'État à l'économie.

5. Loi fédérale du 19 juin 2015 sur le dossier électronique du patient

Art. 7

Le présent projet de loi remplace l'expression «identité électronique» mentionnée à l'art. 7 LDEP par «moyen d'identification électronique». Le «moyen d'identification électronique» correspond mieux au concept qui est réglé à cet article. En outre, il s'agit d'éviter toute confusion avec le présent 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

52 FF **2023** 679

53 Celle-ci correspond au guichet virtuel central prévu à la section 4 du projet de loi fédérale sur l'allégement des coûts de la réglementation pour les entreprises (LACRE), FF **2023** 167; cf. message du 9 décembre 2022 concernant la loi fédérale sur l'allégement des coûts de la réglementation pour les entreprises (LACRE), FF **2023** 166 p. 34 s.

tâche soit confiée au secteur privé, sera également respectée dans le domaine de la LDEP.

Avec les modifications prévues dans l'EMBAG (cf ch. 6), la Confédération jette les bases requises. La Confédération 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, dispose désormais que les éditeurs privés de moyens d'identification doivent continuer à être certifiés.

6. Loi du 18 mars 2016 sur la signature électronique[54]

Art. 9, al. 4 et al. 4bis

La 2e phrase de l'al. 4 est abrogée. Toute personne qui demande la délivrance d'une signature électronique doit se présenter en personne. En vertu de l'al. 4bis, 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 17 mars 2023 sur l'utilisation de moyens électroniques pour l'exécution des tâches des autorités

Le présent 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 «moyen informatique» au sens de l'art. 11, al. 1 à 3, LMETA; il se fonde sur l'e-ID et peut donner accès à un service ou à une application. Lorsqu'elle sera utilisée comme moyen d'authentification, l'e-ID atteindra un niveau de sécurité comparable à «substantiel» selon le règlement eIDAS et à un niveau de confiance 3 selon la norme eCH-0170[55].

Le système d'authentification des personnes physiques (service d'authentification des autorités suisses, AGOV[56]) est également à disposition, en tant que moyen informatique, des cantons et des communes. En outre, AGOV 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.

L'exemple du dossier électronique du patient illustre la manière dont l'e-ID peut être utilisée à l'avenir en interaction avec AGOV: après avoir reçu une e-ID, une personne peut utiliser AGOV pour accéder à son dossier électronique du patient. Concrètement, cela signifie que les utilisateurs du dossier électronique du patient peuvent présenter

54 RS **943.03**
55 www.ech.ch > eCH-0170 Modèle de qualité pour l'authentification des sujets V2.0
56 www.agov.ch

l'e-ID comme preuve d'identité numérique et qu'une procédure de login pour l'accès au dossier électronique du patient en est directement dérivée via AGOV.

Pour que cela soit réalisable, les fournisseurs du dossier électronique du patient, appelés communautés de référence, doivent pouvoir se connecter à AGOV en tant qu'application cible (par ex. au moyen des protocoles SAML [Security Assertion Markup Language]) ou OIDC [OpenID Connect]). La participation aux coûts d'utilisation d'AGOV est réglée à l'art 11 LMETA et prévoit une prise en charge proportionnelle des dépenses occasionnées par l'utilisation.

6 Conséquences

6.1 Conséquences pour la Confédération

Afin que l'e-ID puisse être réalisée aussi vite que possible, il est nécessaire que les préparatifs techniques courent parallèlement à la procédure législative. L'objectif attendu et communiqué jusqu'à présent aux milieux politiques, aux entreprises et à la population est que la Confédération soit en mesure de proposer aux habitants de la Suisse et aux Suisses de l'étranger un moyen d'identification numérique et d'autres preuves numériques (par ex. l'extrait du casier judiciaire) de haute qualité dès l'entrée en vigueur de la loi. L'administration fédérale ne peut attendre ce moment pour commencer à élaborer une solution technique. Le Conseil fédéral a proposé au Parlement de lui allouer un crédit de 6,6 millions de francs dans le cadre du supplément I au budget 2023, pour financer durant cette année la réalisation de projets pilotes et le développement de l'infrastructure de confiance de l'e-ID, et un crédit d'engagement de 40,4 millions de francs affecté au pilotage et au développement de cette infrastructure. Les fonds pour 2023 et le crédit d'engagement ont été approuvés par le Parlement le 1er juin 2023.

Le projet e-ID est géré comme un programme avec coordination de projet selon Hermes. Le mandant est l'OFJ. Un comité de programme e-ID, supervisé par le directeur de l'OFJ, coordonne et accompagne la planification des travaux informatiques. Le projet, mené selon la méthode agile, a été classé «projet TNI clé» par le chancelier de la Confédération le 17 avril 2023[57].

Dans le cadre du projet e-ID, il faut mettre sur pied, exploiter et développer un système d'information servant à l'émission des e-ID et une infrastructure de confiance. Au total, les moyens financiers nécessaires pour le développement et l'exploitation de l'infrastructure de confiance, l'émission des e-ID et les projets pilotes seront d'environ 181,9 millions de francs sur la période 2023 à 2028. Sur cette somme, 58,0 millions de francs sont déjà couverts par les fonds disponibles, Le Parlement a approuvé un crédit d'engagement de 40,4 millions dans le cadre du supplément I au budget 2023 pour les engagements sur plusieurs années liés au pilotage et à la mise en place de l'e-ID,

Les besoins supplémentaires pour la finalisation de la mise en place à partir du milieu de l'année 2025 et pour l'exploitation à partir du début de l'année 2026 se montent à

57 www.bk.admin.ch > Documentation > Communiqués > Nouveaux projets TNI clés

123,9 millions environ. A partir de 2029, il faut s'attendre à des coûts avoisinant 24,7 millions de francs par an.

Un crédit additionnel de 15,3 millions de francs est requis pour la clôture du projet (programme e-ID) durant les années 2025 et 2026. Il est nécessaire, d'une part, parce que les fonds demandés dans le cadre du supplément I au printemps 2023 étaient prévus pour couvrir la période allant jusqu'à la mise en service de l'e-ID, et non celle allant du milieu de l'année 2025 à la fin 2026 (7,7 millions). D'autre part, les moyens destinés à AGOV n'ont pas été entièrement pris en compte dans le crédit d'engagement demandé dans le cadre du supplément I (7,6 millions).

Programme e-ID en francs	B 2025	PF 2026	Total
Infrastructure d'émission de l'e-ID fedpol	6 701 500	965 700	**7 667 200**
AGOV/pilotage ePerso	5 600 000	2 000 000	**7 600 000**

Les charges de biens et services liées à l'informatique sont requises par fedpol pour l'appel d'offres public en vue de l'acquisition de la technologie et de l'infrastructure nécessaires au contrôle d'identité en ligne, et pour développement du système d'information du service d'identité de l'État (SID).

De plus, à partir du milieu de l'année 2025 et jusqu'en 2028, deux autres crédits d'engagement sont nécessaires d'un montant de 85,1 millions de francs (64,9 millions de francs pour l'OFJ et 20,2 millions pour fedpol). Ils ne seront nécessaires que jusqu'à ce que les fournisseurs de prestations internes de la Confédération soient en mesure d'assurer eux-mêmes l'exploitation du système.

Nouveau CE pour l'OFJ	B 2025	PF 2026	PF 2027	PF 2028	Total
Prestations de conseil/de tiers (y compris la communication)	100 000	800 000	800 000	800 000	**2 500 000**
Audit/SMSI/certification de sécurité	0	400 000	400 000	400 000	**1 200 000**
Exploitation OFIT; Infrastructure nuagique y c. frais de licence	3 100 000	3 100 000	3100 000	3 100 000	**12 400 000**
Collaborateurs externes pour l'exploitation	7 286 400	6 652 800	5 385 600	5 385 600	**24 710 400**
Dépenses de support externe	2 595 000	2 880 000	810 000	810 000	**7 095 000**
Prestations externe uniques	3 000 000	5 000 000	5 000 000	4 000 000	**17 000 000**
Total	**16 081 400**	**18 832 800**	**15 495 600**	**14 495 600**	**64 905 400**

Un montant de 0,1 million de francs à partir du milieu de l'année 2025 et de 0,8 million par an à partir de 2026 est prévu pour les prestations de conseil et autres prestations de tiers et pour les frais du service spécialisé e-ID, y compris pour diverses mesures de communication. Les dépenses externes pour l'audit, le système de management de la sécurité de l'information (SMSI) et la certification de sécurité s'élèveront à 0,4 million de francs par an à partir de 2026. Les charges de biens et services

et les charges d'exploitation internes s'élèveront à 3 millions par an à partir de 2025 pour le nuage permettant l'exploitation de l'infrastructure de confiance de l'e-ID. Aucun investissement à la charge des actifs immobilisés de l'OFIT n'est nécessaire. À cela s'ajoutent 0,1 million par an de frais de licence pour le portail de gestion des services informatiques .

Les dépenses de support externe de 2,6 millions de francs pour 2025, de 2,9 millions pour 2026 et de 0,8 million par an à partir de 2027, et les dépenses liées aux collaborateurs externes affectés à l'exploitation, de 7,3 millions pour 2025, de 6,7 millions pour 2026 et de 5,4 millions par an à partir de 2027, constituent la dernière partie des charges d'exploitation récurrentes.

Au titre des charges de biens et services et des charges d'exploitation externes uniques, 3 millions de francs supplémentaires sont prévus pour les prestations de service externes en 2025 (sans le support). En raison du nombre croissant de participants à l'écosystème et des développements techniques à l'étranger, il faut s'attendre à des investissements significatifs en 2026 et 2027, raison pour laquelle il faut prévoir 5 millions de francs pour ces deux années et encore 4 millions à partir de 2028.

Nouveau CE pour fedpol	B 2025	PF 2026	PF 2027	PF 2028	Total
Coûts de licence	500 000	1 000 000	1 000 000	1 000 000	**3 500 000**
Charges d'exploitation	380 000	760 000	760 000	760 000	**2 660 000**
Maintenance, support et développement	651 300	1 302 600	1 302 600	1 302 600	**4 559 100**
Dépenses de support externe	1 584 000	3 168 000	3 168 000	1 584 000	**9 504 000**
Total	**3 115 300**	**6 230 600**	**6 230 600**	**4 646 600**	**20 223 100**

Les charges d'exploitation liées à l'informatique pour les années 2025 à 2028 se répartissent en frais de licence pour le système de vérification en ligne de l'identité d'un requérant, estimés à 20 % du prix d'achat, soit 1 million de francs par an (dont la moitié en 2025). Les charges d'exploitation du système d'information du SID s'élèveront à 0,76 million de francs par an (la moitié seulement en 2025). Les dépenses de maintenance, de support et de développement du système d'information, estimés à 15 % des coûts de développement, correspondent à 1,3 million de francs par an (la moitié seulement en 2025). Enfin, les coûts uniques pour le personnel externe chargé du support s'élèveront à environ 1,6 million de francs pour 2025, 3,2 millions pour 2026 et 2027 et 1,6 million pour 2028. Ces postes externes ne seront plus nécessaires à partir de 2029.

Dès 2025, chaque service qui voudra se raccorder à l'infrastructure e-ID devra lui-même disposer des fonds nécessaires pour le raccordement et l'exploitation (par ex. financement du permis de conduite d'élève par les cantons, qui fait aujourd'hui partie des projets pilotes). L'exploitation d'autres moyens de preuves numériques doit également être assurée par les exploitants de ceux-ci.

Dans le rapport explicatif[58] envoyé en consultation avec l'avant-projet de loi, la première approximation des crédits nécessaires (fondée sur l'expérience du certificat COVID-19) était de 25 à 30 millions de francs pour les coûts de projet et de 10 à 15 millions de francs par an pour les charges d'exploitation. Le rapport précisait qu'une évaluation plus précise des ressources nécessaires aurait lieu lors de l'élaboration du message. Ce n'est en outre qu'avec les projets pilotes que l'on a pu déterminer quelles devraient être la forme et l'étendue du support technique.

Le niveau élevé des dépenses pour le support technique destiné tant à l'infrastructure de confiance qu'à l'établissement de l'e-ID explique l'accroissement des dépenses globales. Ces dépenses n'avaient pas encore été prises en compte dans le rapport explicatif. Les charges d'exploitation doivent être réévaluées et éventuellement adaptées dans le cadre des processus budgétaires des années à venir.

6.2 Conséquences pour les cantons et les communes, ainsi que pour les centres urbains, les agglomérations et les régions de montagne

Lors de la consultation, différents participants ont demandé que le processus de vérification nécessaire à l'émission d'une e-ID ne se fasse pas seulement via un canal en ligne, mais aussi via un processus sur site auprès de structures existantes comme les bureaux des passeports ou les services des migrations. Il serait alors possible pour les personnes intéressées de se rendre auprès de l'autorité en combinaison avec la demande d'établissement de documents physiques, ou de prendre un rendez-vous sur place uniquement pour l'établissement de l'e-ID.

Sur la base des expériences internationales et d'estimations approximatives, l'analyse s'est fondée sur la structure quantitative suivante: 50 % des personnes qui se présentent à l'autorité pour un renouvellement de document d'identité se décident en plus pour l'obtention de l'e-ID; cela représente environ 400 000 cas par an pour les bureaux des passeports et environ 130 000 cas pour les services des migrations. Le nombre de personnes qui se rendent auprès d'une autorité explicitement pour l'e-ID est estimé à 1 % de tous les utilisateurs potentiels de l'e-ID. Pour autant que cette possibilité existe dès l'introduction de l'e-ID, cela générera environ 28 000 rendez-vous sur place la première année, la proportion étant un peu plus élevée au début, puis environ 1000 cas par an à partir de la quatrième année.

Les estimations actuelles du temps nécessaire par cas donnent des coûts supplémentaires de 15 francs pour les vérifications en vue de l'émission d'une l'e-ID en combinaison avec une demande de document d'identité ou de pièce de légitimation. On compte en moyenne 7 minutes supplémentaires par cas auprès de l'autorité. Les coûts d'une vérification sur place uniquement pour l'obtention d'une e-ID s'élèvent à 29 francs. Dans ce cas, on compte en moyenne 14 minutes par cas. En extrapolant en fonction du nombre estimé de cas, on obtient des dépenses d'environ 8 millions de

58 www.fedlex.admin.ch > procédures de consultation > Procédures de consultation terminées > 2022 > DFJP > Loi fédérale sur l'identité électronique et les autres moyens de preuve électroniques (loi sur l'e-ID, LeID)

francs par an. À titre de comparaison, les coûts du canal en ligne sont estimés à un montant de l'ordre de quelques francs par cas. Il s'agit d'estimations provisoires qui sont sujettes à changement après concertation détaillée avec les cantons. Les coûts secondaires (adaptation des infrastructures des bâtiments et des stations, gestion du personnel) ne font pas partie des calculs effectués ici. Les questions relatives à l'acquisition et au financement des éventuelles adaptations nécessaires de l'infrastructure n'ont pas non plus été analysées de manière approfondie.

Les cantons seront libres de percevoir prestations des émoluments pour leurs, dont le montant sera fixé par le Conseil fédéral uniformément pour toute la Suisse. Il n'est pas prévu que la Confédération les indemnise directement.

Après plusieurs séances de travail avec des représentants des bureaux des passeports et des services des migrations, suivies d'une consultation des membres de l'Association des services cantonaux des passeport (ASCP) et de l'Association des services cantonaux de migration (ASM), le principal souci réside dans la gestion des capacités, des ressources et des infrastructures nécessaires. Les coûts secondaires générés par la gestion des capacités (infrastructure des stations, bâtiments, gestion du personnel) n'ont pas été pris en compte dans les calculs présentés ci-dessus. Les adaptations de l'infrastructure n'impliquent pas seulement des questions financières, mais aussi des questions de mise en œuvre (rythme et cycles d'acquisition de crédits et d'infrastructures). En outre, les «années de pointe» historiquement déterminées (2025 et 2026: années de forte demande pour le renouvellement de passeports), les modifications dues à l'introduction prévue de cartes d'identité à puce, une demande accrue due à l'extension des possibilités de caractères spéciaux ainsi que l'introduction d'un permis de conduire numérique, lequel entraînerait une forte demande de l'e-ID, pourraient coïncider avec la phase de lancement de l'e-ID.

Outre la coordination des activités susmentionnées, plusieurs approches pourraient être suivies afin de mieux répartir le nombre de demandes dans le temps et selon les saisons: l'émission de l'e-ID sur site ne devrait pas nécessairement être possible dès le début de l'e-ID; le nombre de rendez-vous disponibles pour les demandes exclusives d'une e-ID pourrait être limité par chaque autorité, avec un quota; une bonne coordination entre le canal en ligne et les vérificateurs sur site peut parer au débordement qui pourrait résulter d'un quota dans le processus d'émission en ligne.

Le processus d'émission en ligne sera le principal canal d'obtention d'une e-ID. Grâce à des mécanismes visant à les orienter dans cette direction, la majorité des personnes intéressées doivent obtenir une e-ID via ce canal. Si les personnes intéressées devaient payer un émolument pour la vérification sur site, cela constituerait un facteur fort pour orienter les demandes vers le canal en ligne qui, lui, serait gratuit. L'expérience montre que les prestations des autorités qui sont gratuites sont volontiers sollicitées.

Les dépenses liées à l'émission sur site pourront être prises en charge par les cantons ou par les requérants eux-mêmes. Les cantons sont en effet des bénéficiaires directs de la mise en place et d'une large utilisation de l'e-ID. Ils pourront toutefois prévoir des émoluments pour cette prestation. Le Conseil fédéral habilitera les cantons à percevoir ces émoluments par voie d'ordonnance.

6.3 Conséquences économiques

La transition numérique 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 communication pour le faire ne manquent pas, il n'est pas encore possible de créer, de gérer et de de présenter des moyens de preuves électroniques qui soient suffisamment fonctionnels et acceptés par la plupart des prestataires. L'infrastructure de confiance de la Confédération vise à combler cette lacune; elle met en place un écosystème qui permet d'émettre, d'utiliser et de présenter de manière sécurisée divers moyens de preuves électroniques. Il s'agit d'un ensemble de normes, 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 LPD. 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 le projet de loi a permis de développer une certaine sensibilité en matière numérique au sein de la population suisse.

6.4 Conséquences sociales

L'identification sûre du partenaire lors des transactions électroniques permet de réduire ou d'empêcher les cas d'abus, augmentant ainsi la confiance sur Internet. L'abus sur Internet se fonde souvent sur l'impossibilité d'identifier son interlocuteur de façon sûre. Il n'est pas possible actuellement de différencier les expéditeurs de *spams* des expéditeurs fiables ni de les placer devant leurs responsabilités. Dans les cas d'hameçonnage, les expéditeurs de courriels se font passer pour quelqu'un qu'ils ne sont pas, par exemple pour la banque du destinataire, et peuvent causer des dommages importants. Les moyens d'identification électronique reconnus contribuent à protéger l'identité de leurs titulaires dans une société mondialisée et fortement interconnectée. Usurper l'identité d'une personne et en faire une utilisation potentiellement problématique devient bien plus difficile.

Des dispositions techniques permettront, lors de la présentation de l'e-ID ou d'un autre moyen preuve électronique, de ne pas toujours devoir transmettre à son interlocuteur toutes les données qu'elle contient et, par exemple, de renoncer à une telle transmission. Son titulaire doit être libre de communiquer tout ou partie des informa-

tions qu'elle contient. La sphère privée est ainsi mieux protégée puisque certaines informations ne doivent plus absolument être communiquées.

En outre, le projet de loi prévoit des restrictions en ce qui concerne l'utilisation de l'e-ID par les vérificateurs; ceux-ci ne peuvent demander au titulaire d'une e-ID de leurs transmettre des données personnelles que sous certaines conditions. Le projet de loi vise ainsi à limiter le recours injustifié à l'identification électronique par les vérificateurs.

6.5 Conséquences environnementales

Ce projet n'a pas de conséquences directes sur l'environnement. Passer de transactions physiques à des transactions électroniques permettrait d'économiser des ressources et aurait par conséquent des répercussions positives sur l'environnement. Par exemple, l'encombrement des infrastructures de transport qui résulte de la nécessité de se présenter en personne pourrait être évité.

La consommation énergétique de l'infrastructure de confiance sera comparable aux autres infrastructures informatiques qui ont déjà été mises en place par la Confédération. En outre, dans le cas où la solution technique de mise en œuvre se fonderait sur technologie *blockchain*, l'utilisation du mécanisme de validation des blocs appelé «preuve de travail» (*proof of work*), connu pour sa forte consommation énergétique, peut été considéré comme exclue pour la mise à disposition de l'infrastructure de confiance.

7 Aspects juridiques

7.1 Constitutionalité

La compétence de régler les e-ID et l'infrastructure de confiance découle des art. 38, al. 1, 81, et 121, al. 1, Cst. Pour plus d'informations, voir le ch. 5 (préambule).

7.2 Compatibilité avec les obligations internationales de la Suisse

Le projet de loi est compatible avec les obligations internationales en vigueur. Lors de son élaboration, le Conseil fédéral a veillé à ce que l'interopérabilité internationale reste possible. 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.

7.3 Forme de l'acte à adopter

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

Conformément aux art. 163, al. 2, Cst. et 25, al. 2, de la loi du 13 décembre 2002 sur le Parlement[59], l'acte concernant les crédits d'engagement à adopter revêt la forme de l'arrêté fédéral simple (qui n'est pas sujet au référendum).

7.4 Frein aux dépenses

La loi ne contient pas de dispositions relatives aux subventions, raison pour laquelle elle n'est pas soumise au frein aux dépenses.

Conformément à l'art. 159, al. 3, let. b, Cst, l'art. 1, al. 2, let. a et b, de l'arrêté fédéral sur les crédits d'engagement alloués à la mise en place et à l'exploitation de l'e-ID doit être adopté à la majorité des membres de chaque conseil dans la mesure où il entraîne des nouvelles de dépenses uniques de plus de 20 millions de francs.

Le crédit additionnel proposé à l'art. 1, al. 1, de l'arrêté fédéral n'est pas soumis au frein aux dépenses, car le crédit d'engagement initial y était soumis et que le montant additionnel ne dépasse pas le seuil des 20 millions de francs.

7.5 Conformité aux principes de subsidiarité et d'équivalence fiscale

Ni le partage des tâches prévu, ni leur exécution ne violent le principe de la subsidiarité ou 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 ne sont pas encore chiffrables.

7.6 Conformité à la loi sur les subventions

Le projet de loi ne prévoit pas d'aides financières ni d'indemnités.

7.7 Délégation de compétences législatives

Le projet de loi se situe délibérément à un niveau d'abstraction élevé; il est substantiellement neutre sur le plan technologique afin de rester ouvert aux changements futurs. La réglementation de certaines questions, parfois même assez importantes, con-

59 RS **171.10**

cernant l'aménagement de l'infrastructure et l'étendue des prestations des différents composants de l'infrastructure ainsi que de l'e-ID, est déléguée au Conseil fédéral.

7.8 Protection des données

Les dispositions du droit de la protection des données (LPD et ordonnances associées) s'appliquent à toutes les parties concernées. 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 aux dispositions applicables aux organes fédéraux. Le présent projet de loi ne contient pas de renvois aux dispositions pertinentes de la LPD, afin d'éviter des répétitions et d'assurer la clarté lors de l'interprétation.

La protection des données est un des buts de la loi, dans son champ d'application. L'art. 1, al. 2, let. a, s'aligne d'ailleurs sur le texte de l'art. 7, al. 2, LPD et précise également aux ch. 1 à 4 comment ce but 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» (21.3124, 21.3125, 21.3126, 21.3127, 21.3128 et 21.3129) qui ont été déposées par tous les groupes parlementaires après le rejet de l'ancien projet de loi lors de la votation du 7 mars 2021. Les motionnaires ont demandé que l'identité électronique étatique respecte certains principes: prendre en compte la protection de la vie privée dès la conception du produit, ne collecter que les données nécessaires et enregistrer celles-ci de manière décentralisée (par ex. auprès de l'utilisateur en ce qui concerne les données d'identification). L'art. 1, al. 2, let. a, 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, du 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. Avec l'emploi de cette notion, le législateur vise un niveau élevé de sécurité et de protection des données grâce à des procédures avancées. L'art. 1, al. 2, let. d, précise par ailleurs que la loi vise à assurer que l'évolution technologique liée aux moyens de preuves électroniques n'est pas restreinte inutilement. Le projet de loi est substantiellement neutre au niveau technologique; il ne règle le choix de la solution technique que lorsque cela est absolument nécessaire pour atteindre les objectifs législatifs.

L'infrastructure de confiance mise en place par le projet de loi se fonde sur les principes énumérés à l'art. 1, al. 2. Les composants principaux de cette infrastructure sont réglés à la section 2. Il s'agit du registre de base (art. 2), du registre de confiance (art. 3), de l'application pour la conservation et la présentation des moyens de preuves électroniques (art. 7) et de l'application pour la vérification des moyens de preuves électroniques (art. 8). Le registre de base et le registre de confiance ne contiennent pas 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 preuves électroniques sont uniquement communiquées entre l'émetteur, le titulaire et des vérificateurs, sans intermédiaire. 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

preuves électroniques émis sont utilisés, 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. Le projet de loi prévoit que les données personnelles générées lors de la consultation des registres de base et de confiance ne peuvent être enregistrées que dans les buts prévus à l'art. 57*l*, let. b, ch. 1 à 3, LOGA. Elles peuvent être analysées sans rapport avec des personnes dans les buts prévus à l'art. 57*l*, let. b, ch. 1 à 3, LOGA.

L'art. 14 énumère les données qui feront partie d'une e-ID. Il s'agit des données d'identification personnelles (al. 1) et des données concernant l'e-ID (al. 2). Les données d'identification personnelles du titulaire sont les suivantes: le nom officiel, les prénoms, la date de naissance, le genre, le lieu d'origine, le lieu de naissance, la nationalité, la photographie et le numéro AVS. Il s'agit de données disponibles dans les registres officiels de l'État auxquels fedpol à accès en vertu de l'art. 25, al. 3. En sus des données d'identification personnelles, une e-ID contient des données 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 de validité, du document d'identité ou de la pièce de légitimation ayant servi lors de son émission (y compris son type et sa date de validité) et des indications relatives à la procédure d'émission. En outre, l'e-ID peut contenir des données supplémentaires dans la mesure où celles-ci sont incluses dans le document d'identité du titulaire (par ex. le nom du représentant légal, le nom d'alliance ou le nom d'artiste).

Le projet de loi prévoit des règles précises permettant à fedpol de gérer un système d'information pour l'identification des requérants. L'art. 25, al. 1, définit la nature, le contenu et la finalité de ce système. L'art. 25, al. 2, énumère les types de données qui y sont enregistrées: les données concernant les e-ID visées à l'art. 14, al. 2, les données relatives à la procédure d'émission (nécessaires à des fins de support technique et de statistique ou d'enquête) ainsi que les données liées à la révocation des e-ID.

Les données d'identification personnelle sont consultées directement dans les registres fédéraux et ne sont pas sauvegardées dans le système d'information de fedpol (cf. art. 25, al. 4). L'art. 25, 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.

L'art. 16, al. 3, du projet de loi constitue une base légale au sens formel permettant à fedpol de collecter des données biométriques pour effectuer une comparaison du visage de la personne et de la photographie visée à l'art. 14, al. 1, let. h. Cette démarche est nécessaire afin de s'assurer que l'image faciale enregistrée du requérant lors du processus d'émission correspond bien à celle contenue dans les registres fédéraux ISA, SYMIC ou Ordipro.

L'art. 22 introduit des restrictions importantes concernant le traitement des données personnelles contenues dans l'e-ID par les vérificateurs. Ceux-ci peuvent demander aux titulaires de leur transmettre des données personnelles contenues dans l'e-ID à des fins de vérification de leur identité ou d'un aspect de leur identité pour des raisons de fiabilité de la transaction ou lorsque cela est requis par la loi. En cas de violation de ces exigences, l'OFIT l'indique dans le registre de confiance et peut exclure du registre de confiance le vérificateur fautif. Des délais de conservation différents sont

prévus à l'art. 26 pour trois types de données contenues dans le système d'information de fedpol. Les données concernant les e-ID demandées et émises et les indications relatives à la révocation des e-ID sont conservées pendant 20 ans à partir de la date de demande ou d'émission de l'e-ID (al. 1, let. a). Les données relatives à la procédure d'émission (y compris les données biométriques), qui sont requises à des fins d'enquête concernant l'obtention frauduleuse d'une e-ID sont conservées cinq ans après la date d'expiration de l'e-ID (al. 1, let. b). Toutes les autres données sont détruites 90 jours après leur enregistrement dans le système (al. 2).

Enfin, le Conseil fédéral se voit également déléguer, à l'art. 32, let. e, la compétence de régler par voie d'ordonnance 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.