

Département fédéral de
justice et police DFJP
Mme la Conseillère fédérale Simonetta Som-
maruga
Bundesrain 20
3003 Berne

Par e-mail à: copiur@bj.admin.ch

Zurich, le 29. Mai 2017

Loi fédérale sur les unités d'identification électronique (loi eID) Consultation

Madame la conseillère fédérale,
Mesdames, Messieurs,

Au nom de Swico, nous vous remercions de la possibilité qui nous est offerte de vous présenter nos réactions à l'avant-projet relatif à la Loi fédérale sur les unités d'identification électronique (loi eID), et vous remettons la présente prise de position.

1. Légitimation et intérêt

Swico est l'organisation des fournisseurs du secteur des TIC en Suisse. Swico représente les intérêts de 450 fournisseurs TIC qui occupent 56'000 personnes et réalisent un chiffre d'affaires annuel de CHF 40 milliards.

Swico est co-fondatrice de l'association Swiss Data Alliance. Swiss Data Alliance milite en faveur d'une politique de données tournée vers l'avenir, afin de permettre aux données de développer leur plein potentiel innovant en Suisse. L'élément clé d'une infrastructure de données fonctionnelle est une preuve d'identité électronique émise par l'Etat.

L'introduction d'une preuve d'identité électronique aura des conséquences directes sur l'ensemble du secteur des TIC et sur les secteurs apparentés. Nos membres sont donc directement et tout particulièrement concernés, ce qui justifie pleinement la présente prise de position de Swico.

2. Contexte

2.1 Demande de remaniement

Swico se rallie à la prise de position de Swiss Data Alliance, et particulièrement à la constatation du fait que le projet présenté par le Conseil fédéral et le concept qu'il présente (en l'occurrence le «Concept 2016» de l'OFP «Moyens d'identification électronique (e-ID) reconnus par l'Etat») ne vont pas dans le bon sens. Nous demandons donc, au vu des considérations qui suivent, le renvoi du projet pour réexamen.

2.2 Besoin d'un document d'identité numérique

Pour un grand nombre de prestations de service, le numérique requiert notre identification en tant qu'utilisateur. Quelques indications sur la personne – une adresse e-mail valide ou simplement un numéro de carte de crédit par exemple – suffisent parfois. Dans d'autres cas cependant, les informations nécessaires doivent être certifiées par une autorité publique, parce que l'application est particulièrement sensible. Citons par exemple le dossier électronique du patient, le vote électronique ou encore un extrait du casier judiciaire. A l'instar du monde analogique, un document officiel permettant de prouver notre identité est alors requis.

2.3 Confiance dans la preuve d'identité fournie par l'Etat

Comme le constate le rapport explicatif relatif au projet mis en consultation, l'Etat jouit, à tous ses échelons, d'une confiance particulière quant à l'exactitude des données relatives aux personnes (voir rapport p. 7).

Dans le monde analogique, l'Etat a mis en place depuis longtemps des institutions souveraines et des procédures nous permettant d'obtenir un document d'identité officiel de ce type. La crédibilité des documents d'identité suisses, et notamment du passeport suisse, est légendaire et sert de base à de nombreuses transactions d'affaires. Nous faisons confiance au passeport suisse parce qu'il est émis par l'Etat et non par une entreprise ou une organisation privée. La crédibilité et la confiance sont également une condition *sine qua non* des relations d'affaires dans le monde numérique. Cependant, nous savons que cette confiance ne va plus toujours de soi pour les prestations de service numériques. Nous devons sans cesse remettre en question la mise à disposition de données personnelles et la raison pour laquelle nous y procédons, et garder à l'esprit le risque que nous encourons à cette occasion. La situation est particulièrement critique lorsque le document d'identité officiel requiert notre identité électronique. Dans ce cas, nous ne pouvons nous contenter de moins que le plus haut niveau de confiance, pour nous-mêmes comme pour le prestataire. A l'instar des documents d'identité analogiques, la preuve officielle de l'identité électronique doit donc rester du ressort exclusif de l'autorité publique. C'est la seule façon de garantir le niveau maximal de confiance et de crédibilité requis par certaines opérations électroniques. Nous ne voulons pas avoir accès à notre dossier électronique de patient avec un titre de transport, et ne voulons pas non plus accéder à notre dossier fiscal avec une attestation bancaire. Nous ne souhaitons pas recevoir un document d'identité électronique émis par un détaillant ou une assurance, mais exclusivement par l'Etat.

3. Quant à l'avant-projet en particulier

L'avant-projet relatif à la Loi fédérale sur les unités d'identification électronique (loi eID) propose de déléguer à des entreprises et à des organisations qui auront fait l'objet d'une certification préalable la fourniture d'identification électronique, tâche qui était jusqu'à présent du ressort de l'Etat. Swico est d'avis que ce concept est voué à l'échec. Aussi crédibles que soient les entreprises et organisations demandant à obtenir l'homologation nécessaire en tant qu'organisme émetteur de documents d'identité électroniques officiels, les utilisateurs ne leur accorderont jamais la même confiance qu'à une autorité publique qui effectue ces tâches de manière souveraine. Or, le succès du passeport électronique suisse repose sur cette entière confiance, condition *sine qua non* du succès de l'économie et de l'administration numériques en Suisse. Dans de nombreux domaines, l'économie apporte de meilleures solutions que l'Etat. La tâche souveraine de l'émission de documents d'identité analogiques ou électroniques n'en fait pas partie.

Nous émettons notamment les critiques suivantes quant à l'avant-projet:

3.1 Focalisation erronée

L'avant-projet ne définit pas de manière suffisamment précise la notion de «service de fourniture d'e-ID». Il importe que l'Etat n'offre pas de services réservés à l'économie privée («services utilisateurs»). Il doit se limiter à son domaine central strictement défini. Cependant, ce domaine central est une tâche relevant de la responsabilité des pouvoirs publics.

3.2 Préciser le terme «e-ID»

La question de l'élaboration d'un système e-ID distinct sous la forme d'un nouveau «registre» n'a nullement été tirée au clair. Il est possible qu'un simple service de requête basé sur des registres existants soit mis en place.

3.3 L'e-ID ne doit pas être un numéro

Par ailleurs, la description d'un e-ID est incomplète. Il est impératif de signaler que – pour des raisons de protection des données et de protection du citoyen au sein de l'Etat notamment – l'e-ID émis par l'Etat ne doit surtout pas être un numéro. Des numéros uniques, à validité limitée dans le temps, et nouvellement générés pour chaque nouvelle transaction (codes d'identification) doivent pouvoir être générés; mais il serait inopportun d'introduire l'e-ID sous la forme d'un numéro personnel central permanent.

3.4 Des numéros structurels systémiques ne doivent pas être communiqués

Avec le «numéro d'enregistrement de l'e-ID» (numéro d'identification univoque attribué à une personne), l'avant-projet s'engage sur la mauvaise voie. S'il s'avère réellement nécessaire, un nouveau registre devrait bien être identifié à l'aide d'un numéro et ce, pour chaque nouvelle requête saisie avec le NAVS13 (à partir des registres ISA, SYMIC et Infostar, ainsi que ZAS-UPI le cas échéant). Ce numéro pourrait très bien être désigné comme «numéro d'enregistrement de l'e-ID». Le numéro d'enregistrement de l'e-ID ne serait cependant qu'un numéro d'ordre technique réservé à l'usage interne (administration), dans le cadre de la gestion et de la mise en place du système e-ID. Cette indication ne doit pas être communiquée à

l'extérieur, d'autant qu'une telle communication n'est en rien nécessaire pour assurer le fonctionnement du système e-ID.

3.5 Incertitude juridique quant à la souveraineté des données

Du point de vue de l'économie, il convient ensuite de souligner que l'art. 10 de l'avant-projet pourrait avoir des répercussions importantes sur les jeux de données déjà détenus par les entreprises privées. En effet, si une entreprise s'inscrivait comme FI aux termes du concept prévu par l'avant-projet, elle devrait assumer le risque de ne plus pouvoir exploiter une grande partie de ses données, dans la mesure où celles-ci correspondent au catalogue de l'art. 7: comment délimiter le jeu de données existant par rapport aux données collectées dans le cadre d'activités de «FI»? L'art. 10 s'avérera soit un tigre de papier, soit un concept aux effets désastreux.

3.6 Perte de temps

En fin de compte, le concept de l'avant-projet laisse craindre que la Suisse ne dispose pas d'un standard unique avant longtemps (notamment en raison de la fragmentation du marché), ce qui, au vu de la numérisation qui bat déjà son plein dans notre pays, est inacceptable. Le présent projet de loi freinerait la Suisse, ce qui doit à tout prix être évité. Il faut donc introduire immédiatement un «e-ID pour tous».

4. Soutien du contre-projet de Swiss Data Alliance

Swiss Data Alliance a rédigé le contre-projet ouvert et constructif ci-dessous, auquel Swico se rallie entièrement:

4.1 Principes d'un régime alternatif

- La preuve d'identité électronique gérée par l'Etat est une tâche souveraine de la Confédération. Lorsqu'il y est convié, l'Etat a pour tâche de contrôler, au sein de l'administration et pour des tiers, l'exactitude des données d'identification de la personne ainsi que l'authenticité de la personne à identifier.
- L'e-ID géré par l'Etat n'est pas un numéro, mais représente l'ensemble des données gérées par l'Etat et permettant d'établir l'identité d'une personne (comme indiqué à l'art. 7 de l'avant-projet), que l'Etat a contrôlées comme étant caractéristiques d'une personne précise, et a enregistrées dans les registres tenus à cet effet. Lorsqu'une application émet la demande, le système d'e-ID étatique ne requiert pas de numéro uniforme pour une personne en particulier, mais uniquement un code de transaction que la personne à identifier lui transmet.
- La Confédération doit émettre et gérer l'e-ID étatique. La crainte de la Confédération de ne pas pouvoir suivre le rythme de l'évolution technologique ne constitue pas une raison valable lui permettant de nier sa compétence dans la confirmation de l'e-ID. L'argument relatif aux coûts (Rapport explicatif relatif à l'avant-projet, chiffre 1.3.1) n'est pas convaincant.
- Sourçage pour le système d'e-ID: la Confédération devrait envisager un partenariat public-privé ou mandater un fournisseur pour l'exploitation du système étatique d'e-ID. Des

systèmes comparables existent déjà dans l'environnement d'émission de documents d'identité (notamment dans le contexte de la loi sur les documents d'identité). Des services à valeur ajoutée sont disponibles en dehors du sourcing. Chacun (également des fournisseurs avec lesquels la Confédération collabore) peut offrir pour son propre compte, à ses propres risques et à son propre avantage ce type de services à valeur ajoutée.

- Spécification du système d'e-ID: le système qui doit être exploité par la Confédération comprend des interfaces de données vers les registres de personnes existants, des éléments de sécurité, une interface externe (API) et un service permettant de contrôler les données d'identification de la personne et leur affectation à une personne précise (authentification).
- Spécifications de l'interface (API, voire un accès Web éventuel) et conditions d'utilisation: Swico soutient les suggestions émises par Swiss Data Alliance dans ce contexte, en l'occurrence l'examen approfondi de la mesure dans laquelle les prestataires de services recourant à l'e-ID doivent s'engager dans le cadre d'un contrat administratif à respecter certaines conditions d'utilisation de l'interface.
- Documents d'identité: en complément du système d'e-ID, mais uniquement sous la forme d'un add-on, les documents d'identité peuvent être émis avec des données d'identification de la personne lisibles par une machine. La connexion à des documents d'identité est une extension et non le contenu principal d'un système d'e-ID fonctionnel de la Confédération.

Swiss Data Alliance a joint en annexe à sa prise de position une ébauche de solution pour l'e-ID généré par l'Etat, qui indique comment mettre en œuvre techniquement les réflexions présentées. Nous y faisons entièrement référence.

4.2 Quant à la base légale en particulier

La question se pose de savoir si l'élaboration du système d'e-ID requiert la création d'une base légale formelle. Dans la mesure où le système d'e-ID ne comprend qu'un simple service de requête sur un registre existant, il peut être envisagé que les lois en place sur les registres servent de base pour une ordonnance du Conseil fédéral (loi sur les documents d'identité, loi sur les étrangers, loi fédérale sur le système d'information commun aux domaines des étrangers et de l'asile (LDEA), Code civil suisse et Ordonnance sur l'état civil, et Ordonnance UPI ainsi que leurs bases légales). Quoi qu'il en soit, cet aspect devrait être reconsidéré (notamment en prenant en compte l'utilité de l'utilisation du NAVS13, de l'interdiction de registres parallèles et du règlement des services de requête exigé dans le cadre du droit de la protection des données). Dans la mesure où une connexion avec le NAVS13 n'est envisagée que pour la base de données ISA, la réglementation de ce seul aspect serait possible dans la loi sur les documents d'identité. Un nouvel acte légal formel ne serait alors pas nécessaire et une réglementation par ordonnance pourrait suffire.

Si la «loi e-ID» devait justifier un nouvel acte, il devrait être simplifié et épuré, ce que permettrait en tout cas le contre-projet proposé par Swiss Data Alliance. En cas d'élaboration d'un nouvel acte, sa justification constitutionnelle ne devrait pas être recherchée seulement dans les art. 95 et 122 Cst. (comme l'indique l'avant-projet), sans quoi la réglementation de l'art. 13 de l'avant-projet ne pourrait pas être justifiée (article ne concernant que le domaine de

l'eGouvernement, difficilement justifiable avec la réglementation du seul point de vue du droit civil). Les dispositions relatives au droit des registres (art. 65 al. 2 Cst.) et les dispositions relatives au droit des documents d'identité basées sur les dispositions relatives au droit civil, au droit des étrangers, au droit d'asile et aux relations avec l'étranger (art. 38, 121 et 166 Cst.) offrent cependant d'excellents compléments. Le cas échéant, il est également envisageable d'invoquer le droit constitutionnel – au sens d'un devoir d'intervention de l'Etat à des fins d'application du droit à la liberté – à la liberté de mouvement (art. 10 al. 2 Cst., au sens du droit constitutionnel à la liberté).

4.3 Quant à la question des contributions en particulier

L'approvisionnement de base par l'Etat devrait par principe toujours être disponible gratuitement. Chaque ayant droit doit recevoir un e-ID sans frais. Si l'utilisateur et l'utilisatrice doivent éventuellement activer l'e-ID dans le système d'e-ID (sous la forme d'une confirmation), l'e-ID est cependant mis à la disposition de chaque ayant droit sans condition.

5. Conclusion

En résumé, il est selon nous indispensable que la constatation initiale de l'identité électronique reste la tâche exclusive de l'Etat. La conception détaillée, notamment en termes d'applications et d'interfaces destinées aux fournisseurs tiers, n'est pas du ressort de l'Etat, mais de fournisseurs d'ID certifiés, qui s'adaptent de manière dynamique au marché. Le citoyen peut alors choisir librement les offres du marché.

Nous vous remercions, au nom de nos membres, de bien vouloir prendre nos suggestions en considération.

Veuillez agréer l'expression de nos meilleures salutations.

Swico

Jean-Marc Hensch
Directeur

Christa Hofmann
Head Legal & Public Affairs