UNE BRÈVE ANALYSE DE LA LOI CONCERNANT LES SERVICES D'IDENTIFICATION ÉLECTRONIQUE

1. PRÉAMBULE

Le 7 mars 2021, le peuple suisse a rejeté par référendum un projet de loi (https://www.fedlex.admin.ch/eli/fga/2019/2311/fr) instituant un service d'identification électronique (SIE/e-ID).

Avant la votation, j'étudiai le texte de loi et rédigeai une notice qui fut distribuée par courrier électronique. Son effet fut très marginal, un certain nombre de récipiendaires ayant réagi signalant que l'argumentation était intéressante, mais qu'ils avaient déjà pris la décision de voter non. Autrement dit, même des personnes dont l'informatique n'est pas le métier avaient décelé le bâclage législatif dans ce qui était soumis à leur appréciation.

2. ANALYSE

2.1 Portée du projet

Manque d'ambition quant aux fonctions, manque de réalisme et de cohérence quant à la mise en œuvre, manque de soin apporté aux aspects de sécurité; la loi soumise à votation concernant l'identité électronique ne me convainc pas du tout.

L'e-ID est un synonyme d'informations personnelles dûment validées à utiliser dans des transactions électroniques (art.21). Pour les prestataires de services Internet, l'intérêt est double :

1. Il permet de relier une personne à de multiples transactions et d'en compiler un profil d'utilisateur.

   L'e-ID standardise cette possibilité pour tous les acteurs Internet en Suisse, sans qu'ils aient besoin de développer leur propre technique d'identification (à l'aide de « cookies » p.ex.), ou de dépendre entièrement de la technique d'identification d'un géant de l'Internet (IDFA d'Apple, p.ex.)

2. Il empêche les usagers de recourir à des pseudonymes pour accéder à des services Internet, puisque l'e-ID est obligatoirement associé à des informations personnelles réelles et vérifiées. Plus question, comme il m'est arrivé de le faire, de créer des comptes avec un nom/prénom bidon et une adresse électronique jetable.

Par contre, et en contraste avec les systèmes utilisés depuis plusieurs années p.ex. en Estonie, Lettonie ou Espagne, l'e-ID ne fournit pas un service d'identification à valeur juridique :

- Il n'est établi aucune équivalence juridique et aucun lien entre l'e-ID et d'autres formes de vérification d'identité (passeport, carte d'identité, permis de conduire, certificat d'origine…)

  Ainsi, pour conclure un abonnement de téléphonie mobile, il faut de nos jours présenter une carte d'identité. Peut-on utiliser l'e-ID comme substitut ? Dans l'état de la loi proposée, rien ne permet de l'affirmer.

- La loi ne contient pas de dispositions concernant une association entre l'e-ID et une signature numérique qui permettrait d'effectuer des actes juridiques par voie électronique (p.ex. conclusion de contrats).

- Le vote par Internet a déjà fait l'objet de réalisations pilotes et de bien des discussions en Suisse; le projet de loi est muet à ce sujet.

L'e-ID apparaît donc comme étonnamment en retard par rapport aux systèmes d'identité électronique introduits dans les pays susmentionnés. L'organisation éclatée de la gestion des e-ID explique en partie cette limitation.

2.2 Rôles et responsabilités des différents acteurs

La loi part du principe que la gestion de l'e-ID s'effectue par un mécanisme de marché, dans lequel plusieurs techniques compatibles sont proposées aux prestataires de services, les usagers demeurant libres de demander et d'utiliser un e-ID ou pas. Ceci n'est pas réaliste.

Une gestion remplissant les conditions de fiabilité, performance et sécurité, requiert des ressources (infrastructure, personnel, émoluments à EIDCOM et FedPol art.31)

Or le mode de rémunération des fournisseurs d'identité n'est pas spécifié. Soit les prestataires de services doivent payer – et ils ne le feront que s'ils y trouvent des avantages supérieurs à leurs systèmes existants. Soit les usagers doivent passer à la caisse, et alors on peut penser qu'ils renâcleront.

La conséquence la plus probable est que seuls de gros acteurs qui peuvent prendre à leur charge les frais de gestion d'e-ID et qui ont un intérêt à sa diffusion finiront par s'imposer en les fournissant gratuitement : Google, Facebook, Apple, Microsoft (qui lieront l'e-ID d'une façon ou d'une autre à leurs propres systèmes d'identification); ou encore un consortium de banques et de gros distributeurs (Denner, Migros, Coop), qui ont un intérêt à un e-ID pour le suivi des consommateurs et les facilités de paiement électroniques esquivant les cartes de crédit. Dans ce dernier cas, les frais disparaissent dans la masse des commissions bancaires.

Cette deuxième voie est celle suivie en Scandinavie (Danemark, Suède, Norvège), où l'identité électronique, matérialisée sous forme de fichier, carte, ou application pour portable, a été définie par les banques afin de faciliter les paiements électroniques avant de voir son usage étendu à d'autres domaines (accès aux dossiers médicaux, aux services Internet de l'État). En Suède, les frais sont pris en charge par les banques; en Norvège, les frais sont à la charge des usagers – une commission est prélevée par les opérateurs de télécommunications pour chaque authentification.

La loi est incohérente quant aux responsabilités respectives des acteurs privés et de la Confédération.

Les exploitants de services peuvent recourir à l'e-ID pour tout type d'utilisation, sans restriction du domaine d'application (art.21), mais son utilisation est limitée à des missions de service public pour les organismes de l'État (art.16-3). Cette différence de traitement est étrange, d'autant que Confédération, cantons et communes peuvent sous-traiter certaines tâches à des acteurs privés – qui eux disposent automatiquement de l'autorisation d'emploi sans contraintes de l'e-ID.

D'après la loi, la gestion des e-ID relève des privés – mais la Confédération doit gérer les données de base, développer le système informatique pour mettre ces données à disposition des fournisseurs d'identités, et être prête de toute façon à gérer elle-même les e-ID en cas de défaillance de ces fournisseurs (art.10, art.14-5). De surcroît, elle assume les tâches de définir techniquement les niveau de garantie (art.4-4), les modalités de blocage et révocation (art.11-5), les normes et protocoles applicables aux systèmes e-ID et les conditions de sécurité (art.13-4), les modalités de conception des systèmes e-ID (art.15-3), et les interfaces assurant l'interopérabilité (art.18-3).

En d'autres termes, l'État doit avoir les compétences nécessaires pour concevoir les systèmes de gestion d'e-ID, mais est censé laisser leur réalisation et exploitation à des acteurs privés. Il eût été administrativement plus simple, économiquement plus avantageux et techniquement moins compliqué de laisser une entité de la Confédération se charger de mettre en place un système universel de fourniture et de gestion d'e-ID (comme l'on fait d'autres pays).

La liberté de choix des usagers risque elle fort de se révéler fictive : dès le moment où les prestataires de services exigent l'e-ID pour se connecter à leurs services, les usagers seront bien obligé d'en passer par là. L'e-ID risque donc de devenir quasiment obligatoire par la bande – comme le montre l'expérience d'autres pays.

2.3 Sécurité

A noter que la loi prévoit (art.12-2) que les usagers doivent avoir le choix entre l'utilisation du niveau de garantie « faible » et un autre mode d'identification. En pratique cela entraînera la disparition de ce mode « faible ». Pour un prestataire de services, pourquoi se donner la peine de mettre en œuvre l'e-ID si l'on doit de toute façon conserver un autre mode d'accès ? Et si l'on met en œuvre l'e-ID, autant passer au niveau « substantiel » et renoncer à cet autre mode.

Justement, ces niveaux de garantie « faible », « substantiel », « élevé » ne sont pas définis concrètement. Il auraient pu être reliés à des degrés de responsabilité civile en cas de perte des informations utilisateurs ou d'usurpation d'identité, ou à des normes de sécurité (ISO, NIST, BSI…) – mais rien n'est spécifié.

La seule prescription explicite concerne la mise à jour des données associées à un e-ID (art.7) – mais la périodicité des mises à jour (semaine, trimestre, année) semble n'obéir à aucune logique de sécurité.

1. Soit l'exactitude des informations gérées (art.5) est essentielle pour assurer la sécurité des transactions – et alors attendre une semaine pour les mettre à jour (niveau de garantie « élevé ») ou plus est inadmissible, car une usurpation d'identité est dévastatrice déjà dans les 24-48 heures.
2. Soit ces informations ne sont pas indispensables pour assurer la sécurité des transactions, et imposer des périodicités de mise à jour ne remplit aucune exigence de sécurité.

A vrai dire, le type d'information associée à un e-ID ne change jamais (date de naissance), très rarement (nationalité, nom), ou exceptionnellement (sexe). Il en va probablement de même pour les informations supplémentaires d'identification que FedPol pourrait définir (art.5-4) – p.ex. adresse, numéro de téléphone, état civil.

La seule information pouvant justifier d'une mise à jour rapide serait une indication que l'e-ID doit être désactivé (art.11-1) – mais alors il est essentiel que cette mise à jour s'effectue sans délai, et surtout pas après une semaine ou une année. Dans ce cas, la loi devrait spécifier que les modifications des informations personnelles sont prises en compte dès la prochaine transaction faisant usage de l'e-ID, ou 2 heures (p.ex) après mise à jour dans le base de FedPol, au plus tôt de ces conditions.

L'e-ID est un mode d'identification; l'accès à un service requiert encore une méthode d'authentification. Dans l'Internet, celle-ci prend la forme d'un mot de passe ou de codes d'accès – qui authentifient l'usager s'étant identifié par un nom, un numéro de compte – ou un e-ID. En principe, l'identité ne change pas, le mode d'authentification pour la même identité peut changer (parfois à chaque utilisation – p.ex. les accès bancaires par CrontoSign).

Le danger est grand de voir s'imposer la technique dite de l'accès unique (single sign-on) : l'établissement d'une session avec un compte utilisant l'e-ID entraîne automatiquement la connexion à tout autre compte utilisant le même e-ID sans avoir à repasser par un guichet d'authentification.

Cette technique est déjà largement utilisée : bien des sites Internet autorisent la connexion avec les paramètres du compte personnel Google ou Facebook. Elle est considérée comme inacceptable dans les recommandations de sécurité. Pour accéder à des services différents, il faut utiliser une authentification différente, et si possible une identité différente. Avec l'accès unique, le piratage de l'identité d'un seul compte déverrouille l'accès à tous les autres comptes, comme l'ont déjà démontré certains cas spectaculaires. Ainsi, des personnes utilisant l'accès unique pour une batterie de services Google ou Apple ont vu des pirates prendre le contrôle de leur portable, bloquer l'accès à leurs ordinateurs, vider leur boîte aux lettres électronique, effacer leurs fichiers, et piller leur compte en banque.

La loi est parfois présentée comme une façon commode de réduire la multiplicité des mots de passe – mais c'est justement ce qu'il ne faut pas faire !

2.4 Conclusion

Un détail curieux, qui semble indiquer que le législateur n'a pas tout à fait réfléchi aux conséquences de l'e-ID est l'art.11-3. En cas de décès, l'e-ID est invalidé – si l'ordonnance d'application ne prévoit rien de plus, cela risque de poser de sérieux problèmes aux héritiers lorsque les comptes nécessaires pour régler la succession ne sont plus accessibles…

La loi proposée n'est ni chèvre ni chou. L'e-ID n'est pas formellement lié à des outils ayant valeur juridique (preuve d'identité, document de voyage, signature électronique) et donc n'apporte rien d'autre que la possibilité d'un mode d'accès normalisé aux sites Internet. L'organisation hybride supposée produire une multiplicité de prestations d'e-ID innovatrices est compliquée, impose des obligations de compétences et de gestion à l'État mais limite son rayon d'action, et ses bénéfices risquent fort de se révéler illusoires.

Bien sûr, les ordonnances d'application pourraient apporter des précisions (p.ex. concernant les niveaux de garantie), mais elles ne pourront effectuer les nombreux rattrapages nécessaires sans excéder le cadre juridique défini par cette loi. Au mieux, celle-ci est un brouillon à rejeter avec la mention « très insuffisant ».

RÉFÉRENCE

Eduardo Casais : *Une brève analyse de la loi concernant les services d'identité électronique*, areppim AG, Köniz, Suisse, 2021-05-26, 5 pages.

AUTEUR

Eduardo Casais a fait partie de l'équipe élaborant le cahier des charges concernant les aspects de sécurité des équipements IP/ATM à Nokia, et participé au développement de plateformes Internet. Il détient un brevet sur les systèmes de sécurité contrôlés par téléphone mobile.

AREPPIM AG

areppim est actif dans la représentation de données quantitatives pour le Web. Le site http://stats.areppim.com publie des données concernant un large éventail de sujets sous forme de graphiques intuitifs associés à des analyses thématiques.

CONTACT

Courrier électronique : info@areppim.com