



Berne, le 13 mars 2026

Ordonnance sur la communication électronique dans les procédures judiciaires et administratives régies par le droit fédéral (OCEP)

Rapport explicatif relatif à l'ouverture de la procédure de consultation



Condensé

Contexte

Le 20 décembre 2024, l'Assemblée fédérale a adopté la loi fédérale sur les plateformes de communication électronique dans le domaine judiciaire (LPCJ, FF 2025 19, RO 2025 583). Cette loi instaure une obligation de recourir à la communication électronique pour les professionnels du droit. L'obligation vaut en particulier pour les autorités, y compris les tribunaux et les ministères publics, et pour les avocats. La Confédération et les cantons disposent d'un délai transitoire de cinq ans pour instaurer l'obligation dans leurs procédures. La LPCJ prévoit en outre la constitution d'une corporation de droit public chargée de mettre en place, d'exploiter et de développer la plateforme centralisée de communication électronique pour les procédures civiles et pénales et les procédures judiciaires régies par le droit administratif. Elle prévoit également la mise à disposition, par une unité de l'administration fédérale centrale, d'une plateforme réservée aux procédures administratives de la Confédération.

Le délai référendaire relatif à la LPCJ a expiré le 19 avril 2025 sans avoir été utilisé. Le 1^{er} octobre 2025, une partie de la LPCJ¹ a été mise en vigueur. Pour que le reste de la loi puisse entrer en vigueur, les conditions suivantes doivent être remplies :

- constitution de la corporation justitia.swiss (par la Confédération et au moins 18 cantons),*
- autorisation et mise en service de la plateforme justitia.swiss,*
- accessibilité sur une plateforme de tous les tribunaux de la Confédération et des cantons visés par la LPCJ,*
- adoption des dispositions d'exécution de la LPCJ.*

Selon les prévisions, ces conditions seront réunies au plus tôt le 1^{er} janvier 2027.

Contenu du projet

Le projet d'ordonnance porte en particulier sur la délivrance d'une autorisation d'exploiter une plateforme au sens de la LPCJ, sur les moyens d'authentification pour pouvoir utiliser une plateforme, sur les formats et tailles de documents autorisés ainsi que sur le montant et la perception d'un émolument pour la plateforme centralisée.

¹ RS 172.023

Table des matières

1	Contexte	4
2	Grandes lignes du projet.....	5
2.1	Autorisation d'exploiter	5
2.2	Moyens d'authentification	6
2.3	Formats et tailles autorisés pour les documents	6
2.4	Numérisation des écrits papier	6
2.5	Émoluments	7
2.6	Propositions de réglementation non retenues	7
3	Commentaire des dispositions.....	9
4	Commentaire de l'annexe (abrogation et modification d'autres actes)	34
4.1	Abrogation de l'ordonnance du 18 juin 2010 sur la communication électronique dans le cadre de procédures administratives (OCEI-PA).....	34
4.2	Abrogation de l'ordonnance du 18 juin 2010 sur la communication électronique dans le cadre de procédures civiles et pénales et de procédures en matière de poursuite pour dettes et de faillite (OCEI-PCPP)	35
4.3	Ordonnance du 23 novembre 2016 sur la signature électronique	35
5	Commentaire de l'art. 26, al. 5, LPCJ	36
6	Conséquences	37
6.1	Conséquences pour la Confédération	37
6.2	Conséquences pour les cantons et les communes	37
6.3	Conséquences économiques	37
6.4	Conséquences sociales	38
7	Aspects juridiques.....	38
7.1	Sécurité de l'information	38
7.2	Protection des données.....	39

Rapport explicatif

1 Contexte

Le 20 décembre 2024, l'Assemblée fédérale a adopté la loi fédérale sur les plateformes de communication électronique dans le domaine judiciaire (LPCJ, FF 2025 19, RO 2025 583). Cette loi instaure une obligation de recourir à la communication électronique pour les professionnels du droit. L'obligation vaut en particulier pour les autorités, y compris les tribunaux et les ministères publics, et pour les avocats. La Confédération et les cantons disposent d'un délai transitoire maximal de cinq ans pour instaurer l'obligation dans leurs procédures. La LPCJ prévoit en outre la constitution d'une corporation de droit public chargée de mettre en place, d'exploiter et de développer la plateforme centralisée de communication pour les procédures civiles et pénales et les procédures judiciaires régies par le droit administratif. Elle prévoit également la mise à disposition, par une unité de l'administration fédérale centrale, d'une plateforme de communication électronique pour les procédures administratives de la Confédération.

Le délai référendaire relatif à la LPCJ a expiré le 19 avril 2025 sans avoir été utilisé. Le Conseil fédéral a décidé le 19 septembre 2025 de mettre en vigueur au 1^{er} octobre 2025 les dispositions de la LPCJ qui sont nécessaires à la création de la plateforme centralisée au sens de la LPCJ (en particulier les art. 1 à 17). Pour que le reste de la loi puisse entrer en vigueur, les conditions suivantes doivent être remplies :

- constitution de la corporation justitia.swiss (par la Confédération et au moins 18 cantons),
- autorisation et mise en service de la plateforme justitia.swiss,
- accessibilité sur une plateforme de tous les tribunaux de la Confédération et des cantons visés par la LPCJ,
- adoption des dispositions d'exécution de la LPCJ.

Selon les prévisions, ces conditions seront réunies au plus tôt le 1^{er} janvier 2027.

Afin de pouvoir tester en amont la plateforme centralisée, plusieurs projets pilotes au sens de l'art. 13a de l'ordonnance du 18 juin 2010 sur la communication électronique dans le cadre de procédures civiles et pénales et de procédures en matière de poursuite pour dettes et de faillite (OCEI-PCPP)² ont été autorisés. Ces projets pilotes ont permis de recueillir de précieuses informations et ont contribué à optimiser la plateforme centralisée pour qu'elle réponde aux attentes des utilisateurs. Lors de ces projets, aucun problème significatif n'a été constaté.

² RS 272.1

2 Grandes lignes du projet

En adoptant la LPCJ, le Parlement a créé les bases légales qui permettront de mener des procédures judiciaires numérisées de bout en bout. La loi prévoit la gestion électronique des dossiers et l'obligation de communiquer par voie électronique pour les professionnels du droit, en particulier les tribunaux, les autres autorités et les avocats. Le présent avant-projet d'ordonnance sur la communication électronique dans les procédures judiciaires et administratives fédérales (AP-OCEP) a pour principal objectif de mettre en œuvre la LPCJ. Il concrétise les conditions applicables à la délivrance de l'autorisation d'exploiter une plateforme au sens de la LPCJ et la procédure à suivre. Il régit les moyens d'authentification autorisés, les formats admis pour la transmission des documents et la taille des fichiers, la numérisation des documents papier par les tribunaux et autres autorités ou encore la perception d'un émolument. Il reprend en outre quelques règles spécifiques au réseau e-LP³, qui figuraient jusqu'ici dans l'OCEI-PCPP. Celle-ci sera abrogée dès l'entrée en vigueur définitive de la LPCJ. De plus, le projet modifie l'ordonnance du 23 novembre 2016 sur la signature électronique (OSCSE)⁴.

L'AP-OCEP s'applique à l'ensemble des plateformes soumises à la LPCJ, y compris à la future plateforme pour les procédures administratives de la Confédération et à la transmission électronique dans le domaine de la poursuite pour dettes et la faillite. Le cadre technique de la future plateforme de la Confédération n'est pas encore connu à l'heure actuelle. Si l'adoption de règles supplémentaires à l'échelon de l'ordonnance devait s'avérer nécessaire pour assurer son exploitation, ces règles seront élaborées pendant la procédure de consultation ou intégrées à l'ordonnance après son entrée en vigueur par la voie d'une révision. Cela vaut en particulier pour les règles applicables à la répartition des frais d'utilisation de la plateforme au sein de l'administration fédérale.

Pour garantir l'adéquation de l'ordonnance avec la pratique, un groupe d'accompagnement composé de représentants de l'administration fédérale, du Tribunal fédéral, du Tribunal administratif fédéral, du Ministère public de la Confédération, des tribunaux et ministères publics cantonaux et de la Fédération suisse des avocats a suivi les travaux.

2.1 Autorisation d'exploiter

En plus de la plateforme centralisée exploitée par la corporation de droit public et de la plateforme pour les procédures administratives de la Confédération, les cantons auront la possibilité de créer d'autres plateformes au sens de la LPCJ. Conformément

³ e-LP est une norme informatique pour l'échange de données relatives aux poursuites pour dette et à la faillite entre les personnes physiques, les personnes morales de droit public ou de droit privé et les offices des poursuites. Des informations plus détaillées figurent sur le site www.eschkg.ch

⁴ RS 943.032

à l'art. 25 LPCJ, l'exploitation d'une telle plateforme requiert une autorisation du Département fédéral de justice et police (DFJP).

La délivrance de l'autorisation est soumise à différentes conditions concernant le chiffrement et la gestion des clés, les quittances, la protection des données et la sécurité des données ou encore les interfaces. Certaines conditions d'autorisation figurent déjà dans la LPCJ, d'autres découleront de l'ordonnance. Enfin, l'avant-projet prévoit que le DFJP sera chargé de définir dans une ordonnance départementale les exigences relatives aux fonctions et à l'exploitation des plateformes, ainsi que les spécifications techniques et le format de données des interfaces.

Dans le cadre de la mise en œuvre, le DFJP examinera s'il est judicieux d'élaborer une fiche d'information récapitulant l'ensemble des conditions d'autorisation.

2.2 Moyens d'authentification

L'avant-projet prévoit l'identifiant pour les services publics suisses AGOV comme moyen d'authentification. Les personnes qui se trouvent à l'étranger peuvent également recevoir un tel identifiant, moyennant la présentation d'un passeport ou d'une carte d'identité valable.

2.3 Formats et tailles autorisés pour les documents

S'agissant du format, l'avant-projet fait une distinction entre les communications des autorités, les écrits des autres participants à la procédure et les annexes de toutes les parties à la procédure. Les communications des autorités doivent s'effectuer au format PDF/A, toutes les variantes normalisées ISO (de PDF/A-1 à PDF/A-4) étant admises. Les autres participants à la procédure peuvent transmettre leurs écrits au format PDF ou PDF/A. Quant aux annexes, elles peuvent être transmises dans n'importe quel format. Lorsqu'une autorité ne peut pas ouvrir l'annexe qui lui a été transmise, elle peut exiger que la partie concernée la lui transmette dans un format lisible. L'avant-projet contient une liste de formats qui doivent pouvoir être ouverts par l'autorité qui dirige la procédure.

Par ailleurs, la taille des documents est limitée à 2 gigaoctets, ce qui devrait être suffisant pour la plupart des documents transmis. Cette limite est nettement plus élevée que celle qui vaut pour la transmission de documents dans le domaine judiciaire au moyen des plateformes de notification reconnues, le volume utile effectif étant dans ces cas limité à 15 mégaoctets. Si, exceptionnellement, un document est plus volumineux que 2 gigaoctets, il pourra être scindé en fichiers plus petits.

2.4 Numérisation des écrits papier

L'avant-projet prévoit une qualité minimale qui doit être respectée lors de la numérisation des documents papier. Il instaure en outre une obligation pour les autorités de vérifier la qualité des documents numérisés.

2.5 Émolument

L'avant-projet prévoit la perception d'un émolument forfaitaire auprès des cantons et de la Confédération. La Confédération supportera 10 % des frais. Les autres frais seront répartis entre les cantons, proportionnellement à leur population.

Le montant de l'émolument sera fixé sur la base de la planification financière de la corporation de droit public. La corporation devra également tenir compte d'une réserve pour des événements imprévus, limitée à 10 % des frais annuels totaux, afin de garantir sa liquidité.

2.6 Propositions de réglementation non retenues

Renvoi des documents physiques

Lors des discussions du groupe d'accompagnement, il a été proposé de créer une disposition prévoyant que l'autorité ne doive pas renvoyer certains documents physiques, à savoir ceux qui ont été écrits spécifiquement pour elle (une dénonciation par exemple) et qui sont encore en possession des auteurs au format numérique, ou encore les copies de documents pertinents au plan juridique, dont les originaux sont conservés par les auteurs de la requête.

Cette proposition a été rejetée étant donné que l'art. 30 LPCJ ne laisse pas de marge de manœuvre pour prévoir, au niveau de l'ordonnance, que certains documents physiques ne doivent pas être renvoyés.

Envoi sur papier

Lors des discussions, le groupe d'accompagnement a proposé de prévoir la possibilité d'envoyer aux personnes qui ne communiquent pas par voie électronique avec le tribunal ou l'autorité concernée, un tirage papier de l'original numérique en lieu et place d'une décision munie d'une signature manuscrite, les lois de procédure ne prévoyant pas que les signatures des membres des autorités doivent être manuscrites.

Dans l'annexe consacrée aux autres actes modifiés par la LPCJ, toutes les dispositions qui prévoyaient jusqu'ici une signature par l'autorité ou le tribunal ont été complétées par l'expression « si la décision est notifiée sur papier » ou par une formulation similaire (cf. par ex. art. 238, let. h, du code de procédure civile [CPC]⁵, art. 353, al. 1, let. k, du code de procédure pénale [CPP]⁶, art. 153, al. 3, de la procédure pénale militaire du 23 mars 1979⁷). Aussi, la LPCJ prévoit-elle déjà expressément

⁵ RS 272

⁶ RS 312.0

⁷ RS 322.1

qu'une signature est nécessaire en cas d'envoi papier. La signature électronique qualifiée avec horodatage électronique qualifié conformément à la loi du 18 mars 2016 sur la signature électronique (SCSE)⁸ est assimilée à la signature manuscrite (art. 14, al. 2^{bis}, code des obligations⁹ [CO]). Toutefois, cette signature et l'horodatage électronique ne peuvent pas être imprimés en conservant leur forme. Il n'existe pas de marge de manœuvre permettant de prévoir des règles différentes à l'échelon de l'ordonnance.

Disposition transitoire pour permettre l'utilisation d'IncaMail et de PrivaSphere

Les discussions du groupe d'accompagnement ont également porté sur la possibilité de créer des dispositions transitoires pour permettre d'utiliser encore pendant une durée limitée les plateformes de notification actuellement reconnues.

Les bases légales des ordonnances sur la communication électronique qui figurent dans les lois de procédure seront abrogées lors de l'entrée en vigueur définitive de la LPCJ. Or, il n'est pas possible de compenser le manque de bases légales au moyen de dispositions transitoires figurant dans une ordonnance ; il faudrait pour ce faire des dispositions transitoires à l'échelon d'une loi formelle.

Toutefois, il sied de préciser que les plateformes de notification reconnues jusqu'ici pourront encore être utilisées dans le cadre des procédures pendantes à la date de l'entrée en vigueur définitive. Les différentes lois de procédure contiennent des dispositions transitoires prévoyant l'application de l'ancien droit aux procédures en cours. Il en va de même de la transmission électronique de documents au moyen des plateformes de notification actuellement reconnues. En revanche, une plateforme au sens de la LPCJ devra être utilisée pour les nouvelles procédures.

Par ailleurs, les plateformes de notification reconnues jusqu'ici pourront encore être utilisées conformément à l'art. 6a, al. 4, PA dans sa version révisée par la LPCJ.

Sur la base du système d'attribution de droit prévu à l'art. 24 LPCJ, on peut également envisager le cas de figure suivant : les plateformes de notification actuellement reconnues auront la possibilité d'ouvrir un compte d'organisation sur la nouvelle plateforme et les utilisateurs qui le souhaitent pourront attribuer à la plateforme qu'ils utilisaient jusque-là le droit de consulter et de transmettre des documents à la nouvelle plateforme. Ainsi, ces utilisateurs pourront continuer à utiliser l'une des plateformes de notification actuellement reconnues sans avoir à modifier leurs processus. En revanche, si l'utilisateur est une autorité, un cachet électronique réglementé devra être utilisé en lieu et place de la signature électronique qualifiée (cf. art. 22, al. 2, LPCJ).

⁸ RS 943.03

⁹ RS 220

3 Commentaire des dispositions

Préambule

La LPCJ modifie une série de lois de procédure, d'où un nombre élevé de normes de délégation. Pour conserver une vue d'ensemble, la LPCJ est mentionnée dans le préambule dans sa totalité, plutôt que les articles pris individuellement. Les dispositions des lois de procédure qui sont mentionnées dans le préambule sont celles qui portent sur la communication par un autre moyen que les plateformes prévues par la LPCJ et qui élargissent de la sorte le champ d'application de l'avant-projet.

Chapitre 1 Exploitation et utilisation de plateformes

Section 1 : Champ d'application

Art. 1

Al. 1

Cette disposition définit le champ d'application du chapitre 1 de l'avant-projet. Elle précise à quelles plateformes et procédures s'appliquent les articles qui suivent et qui portent notamment sur l'exploitation et l'utilisation des plateformes et sur les exigences d'ordre technique ou organisationnel. Ces règles sont impératives pour les plateformes citées à l'al. 1.

Al. 2

Les règles énoncées au chapitre 1 valent également pour les autres plateformes, régies par des lois spéciales, dans la mesure où la LPCJ s'applique à ces plateformes et procédures. De nombreuses lois spéciales renvoient déjà à la loi du 20 décembre 1968 sur la procédure administrative (PA)¹⁰ et donc indirectement aux moyens de communication électronique. Si ces renvois comprennent aussi, en raison des modifications apportées par la LPCJ, les plateformes au sens de la LPCJ, alors les plateformes régies par ces lois spéciales sont elles aussi soumises aux règles énoncées au chapitre 1.

Al. 3

L'alinéa précise que les dispositions spécifiques d'autres lois fédérales ou de leurs ordonnances qui divergent de l'OCEP priment cette dernière.

Section 2 : Autorisation d'exploiter

Art. 2 Conditions applicables aux plateformes

¹⁰ RS 172.021

Al. 1

L'alinéa porte sur les conditions à remplir pour obtenir une autorisation d'exploiter une plateforme au sens de la LPCJ. Celle-ci régit en particulier les exigences relatives à la protection et à la sécurité des données (voir les art. 27 s LPCJ). Les plateformes doivent encore remplir d'autres exigences, qui sont détaillées dans l'ordonnance.

Let. a

En raison des exigences découlant de la législation sur la protection des données (art. 8, al. 1, de la loi fédérale du 25 septembre 2020 sur la protection des données [LPD]¹¹) et afin de maintenir la confiance de la population dans le système judiciaire, les plateformes doivent protéger les documents sauvegardés contre tout accès et toute modification non autorisés. La protection à mettre en place inclut des mesures techniques, comme le chiffrement, la gestion des accès et la journalisation des accès et des tentatives d'accès. S'agissant du chiffrement pendant la transmission, voir les explications figurant sous la let. b.

De plus, les plateformes doivent être en mesure de déjouer les cyberattaques, comme les tentatives de piratage ou de manipulation. À défaut de tels mécanismes de défense, la protection des données et la sécurité de l'information pourraient ne pas être garanties. Les plateformes doivent également pouvoir identifier et bloquer les attaques potentielles afin d'assurer la confidentialité des données (empêcher tout accès par des personnes non autorisées) et leur intégrité (empêcher toute modification par des personnes non autorisées).

Let. b

Le chiffrement des données doit être conforme aux normes officielles de l'administration fédérale. En d'autres termes, il convient d'utiliser des algorithmes de type AES-256 ou des méthodes comparables ou plus récentes afin de protéger les données pendant leur transmission et leur sauvegarde. Cela permet de garantir que la communication électronique dans le domaine judiciaire respecte les exigences élevées en matière de sécurité et est compatible avec les normes internationales.

Les plateformes doivent être en mesure d'assurer une communication conforme aux normes de l'administration fédérale en matière de transmission sécurisée. Concrètement, la let. b fait référence à des protocoles de type HTTPS ou TLS, qui permettent de garantir le transfert sécurisé des données. Un aperçu de ces normes peut être consulté sur [chf.admin.ch](https://www.chf.admin.ch) > Transformation numérique et gouvernance de l'informatique > Directives.

¹¹ RS 235.1

Let. c

Les plateformes doivent pouvoir réceptionner et transmettre des documents de 2 gigaoctets. Cette limite devrait suffire dans la plupart des cas. Les documents contenant du texte et les tableaux de calcul n'atteindront pas cette limite, sauf si d'autres médias y sont intégrés. Les photos prises avec un téléphone mobile ne dépassent généralement pas non plus cette taille. Seules les photos prises avec un téléphone ou un appareil numérique récent et enregistrées au format de données brutes et les vidéos peuvent dépasser la limite de 2 gigaoctets.

Les services de messagerie fixent actuellement souvent une limite à 15 mégaoctets pour les pièces jointes. En comparaison, 2 gigaoctets par document sont nettement plus généreux et semblent suffisants, d'autant plus que les documents peuvent être scindés en plusieurs parties, notamment les fichiers vidéo. Pour d'autres fichiers, il faudra parfois recourir à des logiciels d'archivage comme Zip ou 7-Zip pour scinder les documents en plusieurs parties.

Les exploitants de plateformes peuvent accepter de transmettre des documents plus volumineux. Les copies du contenu d'ordinateurs ou de téléphones mobiles confisqués dépasseront en règle générale la limite de 2 gigaoctets. Les appareils confisqués sont par exemple analysés par des laboratoires forensiques puis transmis aux autorités de poursuite pénale compétentes. Ces données peuvent atteindre des centaines de gigaoctets, voire des téraoctets.

Les fonctions standards de la transmission au moyen d'une plateforme ne sont pas axées sur ces cas spéciaux, mais ces données devraient quand même pouvoir être transmises. Pour que ces fichiers puissent être transmis sans devoir être scindés en plusieurs parties, les exploitants de plateformes peuvent consentir à la transmission de documents volumineux par certains utilisateurs.

Le consentement pourra être donné par oral ou par écrit, ou sous réserve d'une clause de non-responsabilité, par exemple. Il sera en règle générale donné par écrit, ou d'abord oralement dans les cas urgents.

Le cas échéant, on pourra donner à l'autorité un accès à une application forensique pour qu'elle puisse consulter l'annexe.

Let. d

Les plateformes doivent permettre aux utilisateurs de supprimer en tout temps les documents qui se trouvent dans leur profil. Cette fonction est importante notamment pour les personnes qui ont une interface utilisateur sur la plateforme au sens de l'art. 19, al. 1, LPCJ et qui veulent faire de l'ordre dans leur boîte de réception ou d'envoi. Le fait de supprimer un document dans un profil n'entraîne pas forcément son effacement sur la plateforme. L'exemple suivant illustre comment fonctionne l'effacement sur le plan technique. Lorsqu'un document est transmis par une autorité à plusieurs parties à la procédure, il n'est sauvegardé qu'une seule fois sur la plateforme centralisée ; les destinataires et l'autorité expéditrice reçoivent une autorisation

d'accès au document. Tant que d'autres parties ont encore un droit d'accès, la suppression d'un document du profil d'une partie n'entraîne que le retrait du droit d'accès au document de cette partie. Celle-ci n'aura plus accès au document, mais l'effacement physique du document n'aura lieu qu'une fois que tous les droits d'accès auront été retirés (automatiquement ou manuellement).

Al. 2

L'al. 2 précise que le DFJP concrétisera les exigences relatives aux fonctions et à l'exploitation des plateformes, y compris aux interfaces, dans le cadre de la compétence d'exécution attribuée au Conseil fédéral. Les limites de cette délégation au DFJP seront détaillées définitivement pendant la procédure de consultation.

Les plateformes doivent proposer des interfaces permettant aux autres programmes de communiquer avec elles. Des tiers pourront ainsi relier leurs applications spécialisées (par ex. les logiciels de gestion) à la plateforme sans encourir de frais supplémentaires. Il sera ainsi possible de transmettre des documents à la plateforme ou de les réceptionner automatiquement. Cette fonction est particulièrement importante pour les utilisateurs professionnels, qui doivent chaque jour envoyer ou consulter des documents. Elle contribue à optimiser les processus et à simplifier la communication avec les autorités dans le domaine judiciaire. Le recours aux interfaces de la plateforme centralisée et de la plateforme au sens de l'art. 6a, al. 2, PA sera gratuit, ce qui contribuera à accroître l'acceptation des plateformes.

Pour assurer une communication électronique sûre et interopérable, le DFJP édictera des prescriptions techniques concernant notamment les protocoles à utiliser (par ex. RESTful APIs, SOAP ou des protocoles de sécurité spécifiques comme TLS 1.3), les prestations à fournir (par ex. temps de réponse) ou encore les directives d'intégration. Ces mesures garantissent que les interfaces seront extensibles, robustes et résistantes aux interruptions. Le DFJP déterminera également le format des données utilisées lors de la transmission, comme XML ou JSON.

La modification du cadre technique applicable aux interfaces et d'autres modifications de l'avant-projet seront déterminées en accord avec les exploitants de plateformes au sens de la LPCJ (par ex. par le biais d'une consultation informelle). La plateforme centralisée proposera ses interfaces gratuitement, conformément au principe énoncé à l'art. 32, al. 1, LPCJ, qui dispose que la corporation perçoit des émoluments uniquement auprès des autorités. À ce propos, le message concernant la LPCJ¹² souligne expressément, au ch. 4.2.2.4, l'importance de ne pas créer d'obstacles financiers à l'utilisation de la plateforme.

Le DFJP examinera s'il est judicieux d'élaborer une fiche d'information qui récapitule l'ensemble des critères et conditions d'autorisation, pour aider les exploitants de plateformes à rédiger leur demande et réunir les documents nécessaires.

¹² FF 2023 679

Art. 3 Procédure d'autorisation

Al. 1 et 2

Le DFJP est responsable de la procédure visant à autoriser des plateformes au sens de la LPCJ. Il est déjà compétent pour autoriser les plateformes de notification, une solution qui a fait ses preuves en pratique. En outre, il est responsable pour les travaux législatifs menés dans le domaine de la LPCJ. Quiconque entend exploiter une plateforme au sens de la LPCJ devra déposer une demande d'autorisation auprès du DFJP. Le requérant devra attester dans sa demande qu'il remplit les conditions fixées. Il devra notamment présenter les documents suivants :

- un concept d'exploitation qui atteste que toutes les conditions préalables sont remplies,
- des documents relatifs aux spécifications techniques de la plateforme,
- les certificats de sécurité qui prouvent que les exigences légales sont remplies, et
- des données sur la structure de l'entreprise du requérant.

Ces conditions visent à garantir que seules seront autorisées les plateformes qui remplissent les exigences élevées de la LPCJ et garantissent ainsi la protection des utilisateurs et l'intégrité de la communication électronique.

Al. 3

Le DFJP est chargé de régler les détails de la procédure dans une ordonnance départementale. Il précisera en particulier quelles données devront être fournies avec la demande. Le contenu de l'ordonnance en question sera élaboré pendant la procédure de consultation.

Al. 4

Compte tenu des progrès de la technique et de l'évolution constante des cybermenaces, l'autorité chargée de statuer sur les demandes d'autorisation sera tenue de vérifier régulièrement si une plateforme remplit toujours les conditions fixées, faute de quoi l'autorisation devra être retirée en dernier recours. Cette règle est nécessaire pour assurer la protection des utilisateurs, l'intégrité du système de communication électronique et la confiance dans les plateformes. Le retrait de l'autorisation ne saurait toutefois être prononcé à la légère. Le DFJP pourra notamment dans un premier temps prendre une mesure moins incisive et imposer à l'exploitant un délai pour rétablir un état conforme aux prescriptions légales. Si les conditions ne sont toujours pas remplies à l'expiration du délai fixé, alors l'autorisation sera retirée.

En cas de retrait de l'autorisation, les cantons qui utilisent la plateforme en question devront rejoindre une autre plateforme sans délai, afin d'éviter toute interruption dans la communication électronique avec les autorités des cantons concernés. La Confédération n'a actuellement pas connaissance de démarches entreprises en vue de développer d'autres plateformes au sens de l'art. 4 LPCJ.

Al. 5

Un tarif horaire de 250 francs sera facturé pour l'examen de la demande et la délivrance de l'autorisation. Les dispositions de l'ordonnance générale du 8 septembre 2004 sur les émoluments (OGE mol)¹³ s'appliquent au surplus.

Section 3 Documents, quittances et apposition d'un cachet

Art. 4 Format des documents

Al. 1

Cette disposition prévoit que les autorités, à savoir en particulier les tribunaux, les ministères publics et les autorités administratives de tous les échelons, indépendamment du fait qu'ils dirigent la procédure ou y participent sous une autre forme, transmettent leurs documents au format PDF/A. La règle concerne les documents créés par les autorités, notamment les jugements, décisions de tout type et lettres d'accompagnement.

Les autorités devront utiliser le format PDF/A (dans toutes ses versions), qui a été développé spécifiquement pour l'archivage des documents, parce qu'elles automatiseront vraisemblablement l'envoi des documents et l'apposition du cachet (voir l'art. 22, al. 2, LPCJ).

Les autres participants à la procédure (qui ne sont pas des autorités qui dirigent la procédure ou y participent) pourront envoyer leurs écrits adressés aux autorités au format PDF ou PDF/A. On ne peut pas présupposer dans leur cas qu'ils recourront à une automatisation du processus, étant donné que toute personne pourra utiliser la plateforme pour envoyer ses écrits à une autorité, pas seulement les utilisateurs professionnels. Le format PDF/A ne doit pas être un obstacle pour les personnes qui prennent rarement contact avec les tribunaux ou d'autres autorités.

Al. 2

Les annexes aux documents pourront être transmises dans n'importe quel format. Dans la mesure du possible, elles devraient toutefois être transmises au format PDF ou PDF/A, vu qu'il s'agit des formats les mieux à même de garantir une interopérabilité et une reproductibilité maximales dans un contexte hétérogène impliquant de nombreux acteurs (tribunaux, ministères publics, autorités administratives, avocats). Par principe, le risque est couru par l'expéditeur : c'est lui qui doit garantir qu'une autorité pourra ouvrir et utiliser l'annexe. Il devra donc se demander (par ex. en raison du devoir de diligence qui incombe aux avocats) si l'annexe qu'il transmet au tribunal ou à une autre autorité pourra être ouverte et utilisée par le destinataire. Les annexes

¹³ RS 172.041.1

pourront être transmises directement à la plateforme, sans devoir être converties au préalable dans un format pouvant être archivé (ZIP ou 7-Zip par ex.).

Al. 3

L'al. 3 établit une liste des formats que les tribunaux et les autres autorités doivent impérativement pouvoir ouvrir. Cette règle tend à éviter qu'une autorité se prévale de l'al. 4 pour demander systématiquement que les annexes lui soient fournies dans un format particulier (par ex. au format PDF). La liste est à dessein très concise et se fonde sur les formats qui peuvent être ouverts par tous les systèmes ou appareils courants (Windows, macOS, Linux, tablettes, smartphones). Il existe parfois différentes versions d'un format donné, comme c'est le cas pour le format PDF/A (versions PDF/A-1 à PDF/A-4). Lorsque le format PDF/A est cité, toutes les versions courantes sont incluses.

Al. 4 et 5

Les autorités fixent aux participants à la procédure un délai approprié pour renvoyer une annexe qu'elles n'ont pas pu ouvrir. Elles peuvent demander que l'expéditeur renvoie l'annexe dans un format donné ou qu'il leur donne accès à l'annexe sous une forme adaptée. Il est également possible que les tribunaux et d'autres autorités énumèrent les formats qu'ils peuvent lire (dans une fiche d'information, par ex.). Ils doivent toutefois respecter le standard minimal fixé à l'al. 3. Des dispositions comparables figurent dans le CPC et le CPP (voir les art. 132, al. 2, CPC et 110, al. 4, CPP).

La raison pour laquelle une autorité ne peut pas ouvrir l'annexe importe peu. Le logiciel nécessaire à la lecture d'un format particulier n'a peut-être pas été installé, ou les prescriptions relatives à la sécurité des données exigent que l'autorité ne puisse ouvrir que des formats donnés. La disposition ne signifie pas pour autant que les tribunaux et autres autorités pourront systématiquement demander que les annexes leur soient remises au format PDF ou PDF/A.

Données structurées

Le besoin existe en pratique de pouvoir envoyer des données structurées. Étant donné qu'aucun format n'est prescrit pour les annexes, les données structurées pourront être transmises en tant qu'annexes.

Les documents à transmettre doivent être munis d'un cachet électronique conformément à l'art. 22, al. 2, LPCJ. Or, les données structurées ne peuvent pas être cachetées et ne peuvent donc pas être transmises sous forme de documents. Les processus de transmission par la plateforme seront vraisemblablement automatisés, si bien que les autorités pourront créer une lettre d'accompagnement munie d'un cachet (au sens de l'al. 1) et transmettre les données structurées sous forme d'annexes.

Jetons

Les jetons et autres identifiants pourront être transmis en tant qu'annexes dans un document à part, vu que le format des annexes n'est pas prescrit. Les jetons pourront également être transmis sous forme de texte, de code QR ou d'une autre manière dans les documents des autorités et des autres participants à la procédure (au sens de l'al. 1).

Solution rejetée : remettre ultérieurement le format d'origine

La question de savoir si une autorité peut, pour des raisons objectives, demander que le format d'origine d'un document lui soit remis a été examinée. On pourrait l'envisager par exemple lorsqu'une partie convertit en PDF des calculs complexes faits sous forme de tableaux et remet ce PDF en tant qu'annexe. Pour l'autorité, pouvoir demander le document sous sa forme d'origine serait un gain d'efficacité parce qu'elle aurait ainsi accès aux formules et à l'appariement de données, ce qui faciliterait le traitement et le contrôle du document. Cette variante a été rejetée pour différentes raisons. Tout d'abord pour des raisons de sécurité juridique : la partie qui remet un acte doit être sûre qu'elle a respecté le délai imparti et qu'elle a remis l'acte de façon conforme, sans que des tâches supplémentaires lui incombent. Le format d'origine peut en outre contenir des informations que la partie ne veut pas transmettre. La conversion en PDF a pour avantage que seule la partie visible est convertie, donc pas de versions précédentes ni de métadonnées qui résultent du traitement du document. Par ailleurs, des documents PDF peuvent en principe être reconvertis dans le format d'origine. La conversion est facile pour les documents constitués uniquement de texte, mais s'agissant de calculs sous forme de tableaux, elle ne porte que sur les valeurs chiffrées et ne comprend pas les formules.

Autre solution rejetée : établir une liste exhaustive des formats admissibles

Il a été envisagé d'établir une liste des formats admissibles pour les annexes. Il existe des formats standards qui peuvent être ouverts par chaque système ou appareil (Windows, macOS, Linux, tablettes, smartphones). Les discussions au sein du groupe d'accompagnement ont toutefois montré qu'une liste de ce type n'était pas pertinente. Il aurait fallu clarifier ce qu'il fallait faire des formats ne figurant pas sur la liste et expliquer pourquoi certains formats équivalents étaient admissibles et d'autres non. Il aurait été compliqué, surtout pour les utilisateurs non professionnels, de se renseigner au sujet des formats admissibles et ces incertitudes auraient nui à l'attractivité de la plateforme.

Art. 5 Quittances

Al. 1

En lisant l'art. 22, al. 4, LPCJ, on pourrait comprendre qu'une quittance doit être délivrée pour chaque document transmis. L'al. 1 précise qu'une seule quittance doit être délivrée lorsque plusieurs documents sont transmis simultanément.

Al. 2

L'al. 2 indique quelles données minimales doivent figurer sur les quittances, à savoir le type de quittance, le nom de l'expéditeur, celui du destinataire et leur adresse sur la plateforme. Si l'expéditeur agit au nom d'une organisation, le nom de celle-ci devra également y figurer. La quittance de réception mentionnera le nom de chaque document transmis, y compris sa taille et sa valeur de hachage. Si certains documents n'ont pas été transmis en raison du contrôle antivirus, leur nom et taille seront également indiqués.

L'heure de la transmission est également un élément important. L'heure indiquée sur la quittance est l'heure effective à laquelle l'acte a été réalisé, et non le début ou la fin d'un délai légal ou procédural. Lorsque, par exemple, une notification est consultée un dimanche, c'est ce moment qui figurera sur la quittance de consultation et qui sera déterminant pour prouver le moment de la notification (voir l'art. 20, al. 2^{ter} s., PA dans la version révisée par la LPCJ et les dispositions analogues dans d'autres lois de procédure). En cas de non-consultation du document, c'est le moment de la transmission indiqué sur la quittance de non-consultation qui fait foi.

Lorsqu'une personne envoie ou réceptionne un document en raison d'une délégation de droits, ce n'est pas son nom qui figurera sur la quittance, mais celui de la personne au nom de laquelle elle agit.

S'agissant de la taille et de la valeur de hachage, il conviendra d'indiquer ces éléments séparément pour chaque document transmis. Il ne faudra donc pas additionner les tailles des documents ni indiquer la valeur de hachage du total de l'envoi. Lorsque plusieurs documents sont envoyés dans un fichier ZIP, c'est la taille et la valeur de hachage de ce fichier, et non ceux des documents qu'il contient, qui figureront sur la quittance.

Si l'antivirus décèle des logiciels malveillants dans un ou plusieurs documents, ces documents ne seront pas transmis au destinataire (voir l'art. 14, al. 5). Ils figureront malgré tout sur la quittance, avec indication du nom et de la taille. On pourra dans ce cas renoncer à la valeur de hachage vu que ces documents n'auront pas été transmis et n'auront donc pas pu être contrôlés quant à leur intégrité.

Il ne sera pas nécessaire de faire figurer le nom de la plateforme sur la quittance étant donné que ce nom découle du cachet électronique apposé.

L'avant-projet ne prévoit pas que les quittances doivent préciser que la transmission a réussi ou a été retardée, voire interrompue. La quittance de réception au sens de l'art. 22, al. 4, let. a, LPCJ n'est délivrée qu'au moment où un document a été transmis. Aucune quittance ne sera donc émise si la transmission n'a pas réussi.

Al. 3 à 5

Pour pouvoir être utilisées dans la pratique, les quittances doivent être facilement compréhensibles, fiables et avoir force de preuve. Parallèlement, elles doivent contenir des données qui peuvent être lues par la machine, afin de permettre que des inscriptions puissent se faire automatiquement dans les systèmes des utilisateurs. Cette double fonction est difficile à traduire dans une seule quittance, raison pour laquelle les plateformes pourront délivrer deux quittances séparées. Lorsqu'une plateforme délivre une quittance lisible par la machine et une autre qui est lisible par l'humain, seule cette dernière devra être au format PDF/A et munies d'un cachet et d'un horodatage électroniques.

Art. 6 Apposition d'un cachet par l'autorité expéditrice

Conformément à l'art. 22, al. 2, LPCJ, les autorités qui dirigent la procédure et celles qui y participent sont tenues d'apposer un cachet et un horodatage électroniques sur leurs documents. Lorsqu'une autorité transmet plusieurs documents, ils devront tous être munis d'un cachet et d'un horodatage. Les documents qui sont déjà munis d'une signature électronique qualifiée ou d'un cachet électronique réglementé avec un horodatage électronique qualifié ne devront pas être cachetés une nouvelle fois.

Les plateformes devront vérifier que l'autorité a apposé les cachets et l'horodatage nécessaires. Si le cachet ou l'horodatage manque, elles refuseront les documents (voir l'art. 22, al. 2, 2^e phrase, LPCJ).

Art. 7 Apposition d'un cachet par la plateforme

Le but premier du cachet est de protéger l'intégrité des documents et plus précisément de vérifier leur intégrité. Le cachet n'empêche pas la manipulation du document, mais permet de vérifier s'il y a eu manipulation.

Il existe plusieurs manières d'apposer un cachet : il peut d'une part être apposé sur le document lui-même. Cette méthode ne fonctionne toutefois pas avec tous les formats de documents. D'autre part, le système peut calculer la valeur de hachage du document à cacheter et l'insérer dans un autre document qui sera, lui, muni d'un cachet. La valeur de hachage figurant dans le document cacheté permet à la personne compétente de vérifier que l'autre document n'a pas été modifié. Les deux procédures aboutissent au même résultat.

Les avocats ont exprimé le souhait que la plateforme ne modifie pas les documents qu'elle transmet. Des craintes ont été exprimées que les autorités ou les participants à la procédure ne puissent plus déterminer clairement quelle est la version du document qui a été remise dans les délais. Or, si le cachet est apposé directement sur les documents transmis, ceux-ci subissent une modification, alors que s'il est apposé dans un document séparé, les documents transmis restent inchangés.

Al. 1

L'al. 1 règle le cas où plusieurs documents sont transmis ensemble. Ce cas sera la règle, étant donné qu'un écrit est souvent accompagné d'annexes. Dans ce cas, la plateforme appose le cachet et l'horodatage sur un document séparé. Cette règle tient compte à la fois des desiderata exprimés par les avocats et du fait que les annexes peuvent, conformément à l'art. 4, al. 2, être remises dans n'importe quel format.

Al. 2

Le document qui est déjà muni d'un cachet ne devra pas être cacheté une nouvelle fois étant donné que le premier cachet suffit pour prouver qu'il n'a pas été modifié.

Consultation de dossiers

Les art. 6 et 7 AP-OCEP ne s'appliquent pas à la consultation de dossiers, vu qu'aucun cachet ni horodatage ne doivent être apposés dans ce cas (art. 22 LPCJ a contrario). L'obligation d'apposer un cachet et un horodatage (art. 22, al. 2 et 3, LPCJ) ne vaut que pour les actes adressés à l'autorité et pour les notifications (voir par ex. les art. 130 ss et 136 ss CPC) ; il s'agit d'actes par lesquels les parties à une procédure remettent de nouveaux écrits ou de notifications par lesquelles les autorités fixent de nouveaux délais. Pour cette raison, il est nécessaire d'apposer un cachet qui garantit l'intégrité des documents et un horodatage qui confirme le respect d'un délai.

Le législateur n'a jamais voulu que les documents à consulter soient également munis d'un cachet. Lors de la consultation d'un dossier, une partie obtient simplement le droit de consulter des documents existants et ne remet aucun nouveau document. Par conséquent, les documents à consulter ne doivent pas être munis d'un cachet. Un horodatage n'est pas non plus nécessaire, étant donné que l'autorité détermine la durée de l'accès aux documents lorsqu'elle autorise la consultation d'un dossier. Peu importe à quel moment la partie consulte le dossier pendant le délai imparti.

Section 4 *Authentification, profils, interfaces et attribution de droits*

Art. 8 *Authentification des utilisateurs*

Al. 1

Il est prévu de n'autoriser que l'authentification au moyen d'AGOV. L'art. 20, al. 2, LPCJ prévoit que le Conseil fédéral désigne les moyens d'identification électronique admis. AGOV répond aux exigences parce qu'il fournit des identités électroniques natives, enregistrées dans le portail de libre-service destiné aux utilisateurs finaux. AGOV fédère également d'autres identités électroniques reconnues, qui peuvent être

utilisées comme identifiant autonome pour les procédures de connexion¹⁴. Étant donné qu'AGOV peut à la fois fournir des identités électroniques à l'issue d'une procédure de contrôle et fédérer des identités électroniques reconnues, il remplit les conditions visées à l'art. 20, al. 2, LPCJ.

Un des avantages d'AGOV est que toute personne détentrice d'un passeport ou d'une carte d'identité valable peut obtenir un identifiant AGOV de niveau 300 (principe d'universalité). Des personnes à l'étranger qui ne possèdent pas un document d'identité suisse pourront donc également participer à la communication électronique en Suisse. Cela concerne plus spécifiquement les avocats de l'Union européenne qui sont également habilités à représenter des parties devant les tribunaux suisses. En cas de communication électronique au moyen de la plateforme, ils ne devront plus élire un domicile de notification physique en Suisse (voir par ex. les art. 11b, al. 1, PA et 39, al. 3, de la loi du 17 juin 2005 sur le Tribunal fédéral [LTF]¹⁵ dans leur version révisée par la LPCJ).

Une personne qui dispose d'une e-ID suisse pourra facilement se procurer un identifiant AGOV au niveau 300. Par ailleurs, l'e-ID suisse devra aussi être acceptée comme moyen d'identification, conformément à l'art. 24 de la loi du 20 décembre 2024 sur l'e-ID (LeID)¹⁶. Il n'est pas nécessaire de mentionner expressément l'e-ID dans l'ordonnance vu l'art. 24 LeID.

D'autres preuves d'identité électroniques pourraient théoriquement encore être admises, mais elles devraient d'abord être intégrées par la plateforme centralisée et le cas échéant par d'autres plateformes, ce qui compliquerait le système et engendrerait des coûts supplémentaires. Vu que toute personne peut en principe obtenir un identifiant AGOV au niveau 300, il n'est pas nécessaire de prévoir d'autres preuves d'identité électroniques.

Al. 2

Si les cantons exploitent d'autres plateformes au sens de l'art. 4 LPCJ, ils doivent également utiliser AGOV comme service d'authentification. Ils peuvent aussi utiliser un autre service de qualité équivalente. Ils devront eux aussi accepter l'e-ID suisse au sens de la LeID comme moyen d'identification.

¹⁴ Voir la page Internet « Informations destinées aux autorités » à consulter sur le site www.agov.admin.ch > Pour les autorités

¹⁵ RS 173.110

¹⁶ FF 2025 20

Al. 3

L'art. 21 LPCJ prévoit que les personnes qui utilisent une plateforme au moyen de l'application d'une autorité n'ont pas besoin de s'authentifier sur la plateforme si l'exploitant de la plateforme les autorise à y accéder directement. Il faudra du temps jusqu'à ce que toutes les autorités qui le veulent aient raccordé leurs applications à la plateforme par une interface. On peut aussi envisager que des autorités plus petites, qui n'utilisent la plateforme qu'occasionnellement, recourent simplement à la connexion Web de la plateforme. Dans ces cas, il sera utile que l'exploitant d'une plateforme puisse également accepter d'autres identifiants (par ex. les fournisseurs d'identité des cantons) garantissant un niveau de protection adapté. L'exploitant ne sera toutefois pas tenu d'accepter ces fournisseurs d'identité.

Art. 9 Profils

Al. 1

Les plateformes doivent permettre de créer plusieurs profils dans un compte utilisateur. Les utilisateurs pourront ainsi agir en différentes qualités sur une plateforme. Une personne physique pourra être soumise à l'obligation d'utiliser la plateforme en tant qu'avocat, par exemple, et vouloir l'utiliser également pour elle-même, indépendamment de son rôle d'avocat. Si cette personne est aussi membre d'un ou de plusieurs conseils d'administration et membre du comité d'une association locale, elle pourra changer de profil et envoyer ou réceptionner des documents dans ces différents rôles.

Al. 2 à 4

Pour éviter que les documents soient envoyés à la mauvaise personne, les profils devront contenir un nombre minimal de données.

Le profil d'une autorité comprendra au moins les données suivantes : le nom de l'autorité, son adresse postale et la désignation du cachet. Les deux premiers éléments servent à identifier l'autorité voulue, alors que le nom du cachet sert un autre but. Lorsqu'une autorité transmet des documents, elle doit les munir d'un cachet électronique. La désignation du cachet dans le profil de l'autorité permettra aux plateformes de vérifier qu'au moins un document est muni du bon cachet (voir l'art. 22, al. 2, LPCJ).

Le cachet est désigné par le champ « nom commun » (*common name*, *CN*) du certificat. Le CN est un élément central des certificats X.509 et sert d'identifiant pour le titulaire du certificat. Son objectif et son utilisation varient en fonction du type de certificat. Dans le cas des certificats SSL/TLS, le CN doit correspondre au nom de domaine du site Internet. S'agissant de documents munis d'un cachet, le nom de l'organisation constitue le CN.

Pour les personnes physiques, il faut indiquer les nom et prénom, l'adresse postale et la date de naissance. Pour les organisations, il faut indiquer son nom ou celui de l'entreprise ainsi que l'adresse postale. Ces données excluent pour ainsi dire une erreur d'acheminement.

Lorsqu'une personne soumise à l'obligation d'utiliser la plateforme crée un profil, elle indiquera l'organisation dont elle fait partie et son adresse postale professionnelle. Il est par ailleurs usuel pour les cabinets d'avocats d'indiquer le nom du cabinet et d'utiliser notamment le papier à lettres officiel.

Les organisations au sens des al. 3 et 4 peuvent être des personnes morales, mais aussi d'autres organisations comme les sociétés simples ou les sociétés en nom collectif. Les cabinets d'avocats sont souvent des sociétés simples ou des sociétés en nom collectif.

Si le profil appartient à une personne physique, l'identité de cette personne devra être confirmée au moyen d'AGOV. Il n'existe pas de processus comparable pour les organisations : le nom de l'organisation et le droit de représentation ne seront pas vérifiés, mais dans le cas d'une organisation, une personne responsable est toujours mentionnée. Lors de la création du profil d'une organisation, la personne physique à qui appartient le compte sera mentionnée. Cet élément pourra être modifié ultérieurement, avec le consentement du nouveau responsable. Les autorités devront vérifier dans le cadre de la procédure, comme elles le font déjà, que l'organisation existe et que le droit de la représenter est valable.

Art. 10 Interface

L'accès par l'interface se fait par un jeton d'API – une clé alphanumérique sûre. Le jeton d'API fonctionne comme un mot de passe numérique généré spécifiquement pour la communication de machine à machine entre des applications ou des services, sans partage de données sensibles liées à l'utilisateur. Ces jetons sont fréquemment utilisés pour garantir des accès contrôlés et sûrs.

La création d'un jeton est assimilable à la délégation de droits à un autre utilisateur, raison pour laquelle ces jetons devront être confirmés régulièrement, faute de quoi ils seront effacés ou désactivés automatiquement.

Art. 11 Attribution et retrait de droits

Le système permet à une personne d'attribuer à d'autres personnes le droit d'envoyer ou de réceptionner des documents en son nom (voir l'art. 24 LPCJ). L'attribution de droits peut avoir des implications notables, raison pour laquelle les utilisateurs devront vérifier ces droits au moins une fois par an.

Si une personne ne confirme ni ne refuse les droits qui lui sont délégués, la plateforme retirera les droits automatiquement trois mois après la dernière demande de confirmation.

Les utilisateurs concernés, à savoir ceux qui ont délégué les droits et ceux qui les ont reçus, seront informés du retrait automatique. Si le retrait n'est pas souhaité, les personnes concernées pourront entreprendre des démarches pour réattribuer les droits. La personne à qui les droits avaient été délégués pourra par exemple demander au délégataire de les lui réattribuer.

Section 5 Protection des données, sécurité des données et contrôle antivirus

Art. 12 Durée maximale de conservation des documents et des quittances

Al. 1

L'art. 22, al. 5, LPCJ fixe un délai minimal de 90 jours au cours desquels les plateformes ne peuvent pas détruire automatiquement les documents transmis et les quittances délivrées. Conformément à l'al. 1, la durée maximale de conservation sera de six mois. Les délais de conservation visés à l'art. 21 de l'ordonnance du 15 novembre 2017 sur la surveillance de la correspondance par poste et télécommunication (OSCPT)¹⁷ sont réservés.

Les documents ne devront pas être détruits exactement à l'échéance du délai de six mois suivant leur transmission. Les plateformes auront, en fonction de leur capacité, quelques heures supplémentaires pour le faire, mais la destruction des documents devrait cependant survenir dans les 24 heures.

Al. 2

Lorsque des pièces de dossier peuvent être consultées sur la plateforme, l'autorité fixe le délai au cours duquel elles seront disponibles. Les plateformes les détruiront automatiquement passé ce délai. Le délai de six mois mentionné à l'al. 1 ne s'applique donc pas dans ce cas.

Solution rejetée

La possibilité de lier la durée maximale de conservation à l'activité ou à l'inactivité des parties à la procédure a également été envisagée. L'idée était d'effacer les documents lorsque plus aucun nouveau document n'a été transmis ou que plus aucun acte n'a eu lieu pendant une certaine période. Cette solution a été rejetée parce que, pour des raisons techniques, les plateformes ne peuvent pas toujours déterminer si le document transmis fait partie d'une procédure en cours ou d'une nouvelle procédure.

¹⁷ RS 780.11

Art. 13 Sécurité des données

L'utilisation abusive d'informations et la perturbation de systèmes d'information sont susceptibles de nuire gravement aux intérêts de la Suisse et aux droits des personnes. L'évolution de la société en société de l'information comporte des risques dont la complexité et le dynamisme vont croissant. En adoptant la loi du 18 décembre 2020 sur la sécurité de l'information (LSI)¹⁸, le Parlement a créé un cadre juridique uniforme, fondé sur des normes internationales, qui régit la gestion et la mise en œuvre de la sécurité de l'information dans les domaines de compétence de la Confédération.

Étant donné que la Confédération est partie prenante à la plateforme centralisée et à la plateforme destinée aux procédures administratives, il semble logique que les exigences en matière de sécurité des données soient régies par la LSI. La Confédération a réuni dans cette loi les principales bases légales applicables à la sécurité des informations et des moyens informatiques de la Confédération, l'objectif étant d'atteindre un niveau de sécurité aussi homogène que possible, qui vaut également pour les plateformes au sens de la LPCJ. L'art. 13 ne s'applique qu'aux cantons, étant donné que les prescriptions de la LSI sont de toute façon applicables à la Confédération.

Le Préposé fédéral à la protection des données et à la transparence (PFPDT) exerce en outre la surveillance relevant de la protection des données sur les plateformes (art. 27, al. 6, LPCJ), ce pourquoi l'art. 8 LPD est également applicable.

Art. 14 Contrôle antivirus

Al. 1

Conformément aux prescriptions applicables à la protection des données et à la sécurité des données (art. 27 s. LPCJ), les plateformes doivent soumettre les documents qui leur sont transmis à un contrôle antivirus. Le « contrôle antivirus » qui figure dans l'avant-projet vise la détection de logiciels malveillants en général. Plus un document est volumineux, plus les ressources engagées pour effectuer un contrôle antivirus sont importantes. Les plateformes peuvent contrôler les documents d'un volume maximal de 64 mégaoctets sans baisse de productivité, raison pour laquelle c'est cette limite qui a été retenue.

Al. 2

Lorsque des documents dépassant 64 mégaoctets sont transmis, les plateformes pourront les scinder en documents de 64 mégaoctets et les soumettre à un contrôle antivirus. Dans ce cas, il y a toutefois un risque qu'un logiciel malveillant se trouve à

¹⁸ RS 128

différents endroits dans un document et que l'antivirus ne le reconnaisse pas si le document est transformé en plusieurs parties plus petites. C'est pourquoi l'avant-projet prévoit que les plateformes devront identifier ces documents en tant que tels. Les destinataires pourront ainsi prendre les mesures de précaution qui s'imposent.

Al. 3

Il existe aussi des situations où des documents contenant des logiciels malveillants sont transmis en connaissance de cause, par exemple lorsque les autorités de poursuite pénale confisquent des ordinateurs ou des appareils mobiles. Les logiciels malveillants contenus dans ces appareils font alors partie des moyens de preuve et ne doivent pas être altérés. L'avant-projet prévoit dès lors que l'exploitant d'une plateforme peut accepter sur demande de renoncer au contrôle antivirus.

L'exploitant pourra y consentir par oral ou par écrit, ou sous réserve d'une clause de non-responsabilité, par exemple. Le consentement pourra être donné pour un seul cas ou pour une durée déterminée ou indéterminée. Il sera en règle générale donné par écrit et pourra être donné d'abord oralement dans les cas urgents.

Al. 4

Si les documents ne sont pas soumis à un contrôle antivirus ou sont soumis à un contrôle restreint au sens de l'al. 2, ils seront identifiés en tant que tels par la plateforme, pour que les destinataires puissent les traiter avec le soin nécessaire.

Al. 5

Si la plateforme constate qu'un ou plusieurs documents contiennent des logiciels malveillants, elle refusera de les transmettre au destinataire. Elle lui remettra uniquement les documents non infestés qui devaient être transmis simultanément. La quittance au sens de l'art. 11 contiendra, à des fins de preuve, la liste des documents qui n'ont pas été transmis, avec indication de leur taille. Le droit de procédure règle déjà la manière dont les actes entachés d'un vice doivent être traités (voir par ex. l'art. 132, al. 1, CPC). Normalement, un délai raisonnable sera fixé pour la remise des documents manquants.

En pratique, cette disposition ne devrait s'appliquer que dans de rares cas, étant donné que la majeure partie des documents sera transmise au format PDF ou PDF/A. Lorsqu'un document PDF est créé avec les outils de conversion usuels, par exemple par la fonction « enregistrer sous » ou « exporter » de Microsoft Office ou par la fonction « imprimer » dans le logiciel PDF24, alors le processus de conversion transforme pour l'essentiel le contenu visible du document en un format statique et élimine les éléments pouvant être exécutés, qui peuvent contenir des logiciels malveillants. Théoriquement, on ne peut pas exclure que des logiciels malveillants soient contenus par exemple dans le système d'exploitation ou dans le pilote d'imprimante PDF et qu'ils soient transférés dans les documents PDF pendant le processus de conversion. Il n'existe cependant pas d'exemple connu de logiciel malveillant de ce type.

Section 6 *Émolument pour l'utilisation de la plateforme centralisée*

Conformément à l'art. 32 LPCJ, la corporation de droit public perçoit des émoluments annuels pour l'utilisation de la plateforme centralisée et le Conseil fédéral peut prévoir des montants forfaitaires. Il découle du commentaire de l'art. 32 LPCJ dans le message que le terme de « forfaits » ne se limite pas aux émoluments, mais porte aussi sur la facturation : le Conseil fédéral peut prévoir, pour simplifier la facturation, que les émoluments ne soient pas prélevés par chaque autorité, mais par le canton ou la Confédération.

Art. 15 *Calcul de l'émolument*

Al. 1

La disposition constitue la base de calcul du montant total de l'émolument annuel. L'émolument couvre les frais d'exploitation et de développement de la plateforme centralisée (principe de la couverture des frais). Il peut également comprendre une réserve limitée à 10 % des frais d'exploitation annuels. Cette réserve sert uniquement à garantir la liquidité de la corporation de droit public (par ex. pour assurer les flux de paiement, des dépenses inattendues, des pics de financement à court terme). Il s'agit bien d'une réserve et non d'une marge bénéficiaire. Il faut par ailleurs déduire du calcul de l'émolument total les recettes provenant des cantons non membres de la corporation, qui paient les prestations auxquelles ils recourent. On évite ainsi que les membres financent des frais qui sont déjà couverts par des tiers non membres (pas de financement double).

Al. 2

Le DFJP fixe le montant annuel de l'émolument en se fondant sur la planification financière de la corporation de droit public. Il le fait tous les trois ans, ce qui augmente la prévisibilité et réduit les charges administratives (le tarif et l'émolument ne seront pas adaptés chaque année) tout en tenant compte de la couverture des frais.

L'émolument est fixé en fonction des paramètres concrets de la planification (budget/planification sur plusieurs années, plan d'investissement et roadmap de développement, calcul entrepreneurial). Ces paramètres répondent à des exigences en matière d'objectivité et de documentation auxquels est liée la décision du DFJP. Cela signifie concrètement que la corporation de droit public remettra chaque année une documentation actualisée au DFJP. Celui-ci fixera l'émolument tous les trois ans dans une décision formelle.

Al. 3

Si le DFJP constate lors de la fixation de l'émolument au sens de l'al. 2 que l'émolument ne couvre pas les frais d'exploitation et de développement ou que la réserve dépasse la limite fixée à l'al. 1, il pourra adapter le montant de l'émolument. L'al. 3 a pour fonction de corriger le rythme trisannuel : si les prévisions se révèlent fausses ou

que les frais augmentent de manière inattendue et que la réserve ne suffit plus, le financement restera garanti. Il en va de même pour le cas où l'émolument serait trop élevé et que la réserve dépasserait la limite fixée.

Solution rejetée : répartition des coûts de mise en place

Selon la planification actuelle, le développement de la plateforme centrale sera achevé lorsque toutes les parties de la LPCJ seront entrées en vigueur – faute de quoi le reste de la loi ne pourra pas entrer en vigueur. Pour ces raisons, l'avant-projet ne porte pas sur le financement des frais de mise en place au sens de l'art. 33 LPCJ.

Art. 16 *Répartition de l'émolument*

La perception forfaitaire de l'émolument implique que l'on détermine d'abord la part qui sera financée par la Confédération et celle qui sera financée par les cantons. Le message concernant la LPCJ¹⁹ présente les statistiques du Tribunal fédéral pour l'année 2020. Compte tenu des procédures menées devant le Ministère public de la Confédération (MPC) et devant les ministères publics des cantons, la part des procédures relevant de la Confédération était de 2,17 %. Entre-temps, le Tribunal a publié les statistiques 2024 :

Nombre de procédures liquidées	Conf.	Cantons	Total
Par les autorités judiciaires	15 090	390 899	405 989
Par le MPC et les ministères publics des cantons	1 646	550 458	552 104
Total	16 736	941 357	958 093
Proportion	1.75 %	98.25 %	100 %

Comparé à l'année 2020, le nombre de procédures liquidées par la Confédération a légèrement diminué. À noter que les procédures pénales administratives de la Confédération et des cantons ne sont pas incluses dans ces statistiques. Leur nombre est difficile à évaluer. Un nombre non négligeable de procédures est à comptabiliser dans le domaine des impôts fédéraux, en particulier celui de la TVA, en matière de douane ou encore en lien avec la Commission fédérale des maisons de jeu.

Il semble approprié de prévoir une participation forfaitaire de la Confédération plus élevée, de 10 %, compte tenu des éléments suivants : d'une part, les tribunaux cantonaux réalisent certains travaux préparatoires pour le Tribunal fédéral, comme la numérisation des requêtes et annexes remises sur papier, d'autre part, la numérisation de la justice entraînera aussi un gain d'efficacité pour la Confédération, difficile à exprimer en chiffres. Le montant plus élevé tient aussi compte du fait que la Confédération joue un rôle de poids dans la corporation, qui est inscrit dans la loi. La convention à conclure pour constituer la corporation de droit public prévoit notamment que la

¹⁹ FF 2023 679 p.18

Confédération sera représentée au comité, l'organe stratégique, avec deux membres sur sept.

Le projet Justitia 4.0 estime que les coûts annuels nécessaires à l'exploitation et au développement ultérieur de la plateforme centralisée se situeront entre 10 et 12 millions de francs. Si la Confédération participe aux frais à raison de 10 %, elle versera entre 1 000 000 et 1 200 000 francs, les cantons supportant les frais restants de 9 000 000 à 10 800 000 francs.

La part de la Confédération sera financée à parts égales par l'administration fédérale et par les tribunaux de la Confédération. La part des cantons sera répartie entre les différents cantons, proportionnellement à leur population.

Ordonnance générale sur les émoluments (OGEmol)

L'OGEmol s'applique dans la mesure où l'avant-projet ne prévoit pas de règles spécifiques.

Solution rejetée : répartition des frais selon l'utilisation effective

Plutôt que de prévoir des contributions forfaitaires en fonction de la population cantonale et du nombre de procédures liquidées par la Confédération, l'émolument pourrait aussi être perçu en fonction de l'utilisation effective de la plateforme centralisée. Celle-ci procède déjà à des statistiques et peut fournir des données détaillées sur son utilisation par les différentes autorités, ce qui permettrait de calculer le montant de l'émolument.

Le prélèvement d'émoluments en fonction de l'utilisation effective pose toutefois un problème, car l'utilisation peut fortement différer d'un canton à l'autre vu qu'il n'y a pas d'obligation légale d'utiliser la plateforme valant pour toute la Suisse. Les cantons introduisant l'obligation avant les autres – ou la Confédération – devraient alors supporter une part des frais beaucoup plus élevée, alors que les cantons recourant plus tard à la plateforme profiteraient de la situation.

Art. 17 Part de l'administration fédérale et du MPC

Al. 1

Le DFJP versera l'émolument dû par l'administration fédérale. Il jouera le rôle de service de paiement central dans les rapports avec la corporation de droit public. Ce principe simplifiera le décompte. Il s'agit des paiements externes et des compétences vis-à-vis de l'extérieur et non de la répartition interne des frais.

Al. 2

Le Conseil fédéral décide de la répartition de la part de l'administration fédérale au sein de celle-ci, à savoir entre les départements, la Chancellerie fédérale et le MPC, et ce pour trois ans. La répartition des frais fait ainsi l'objet d'une décision uniforme

jouissant d'une légitimité politique. Le fait que la répartition soit fixée tous les trois ans contribue également à la sécurité de la planification.

Al. 3

Les départements et la Chancellerie fédérale pourront imputer leur part aux unités administratives centralisées ou décentralisées qui leur sont subordonnées. Les départements pourront ainsi appliquer le principe de causalité à leur échelon. Il s'agit d'une disposition potestative ; les départements et la Chancellerie fédérale ne sont pas obligés de répartir les frais.

Comme aucune unité administrative n'est subordonnée au MPC, il n'y a pas d'imputation des frais dans ce cas.

Art. 18 Part des tribunaux de la Confédération

Al. 1

Le Tribunal fédéral paiera la part de l'émolument qui devra être financée par les tribunaux de la Confédération. Il joue le même rôle que le DFJP pour l'administration fédérale et centralise le paiement de la part relevant de l'ensemble de la juridiction fédérale. Ce principe simplifie le décompte et les paiements.

Al. 2

Le Tribunal fédéral fixera la clé de répartition pour les tribunaux de la Confédération après les avoir entendus, pour garantir l'équité et une bonne acceptation de la répartition. Les règles fixées correspondent d'ailleurs au droit en vigueur : le Tribunal fédéral exerce la surveillance sur la gestion du Tribunal pénal fédéral, du Tribunal administratif fédéral et du Tribunal fédéral des brevets conformément à l'art. 1, al. 2, LTF. Cette surveillance comprend entre autres la surveillance financière, exercée par une planification financière commune portant sur plusieurs années et par l'examen et la discussion des projets de budget et de comptes annuels (art. 3, let. c, en rel. avec l'art. 6, let. a et b, du règlement du 11 septembre 2006 sur la surveillance par le Tribunal fédéral²⁰).

Contrairement à ce qui est prévu pour l'administration fédérale, aucune fréquence n'a été déterminée pour la répartition. Celle-ci pourra par conséquent être adaptée avec davantage de flexibilité. Il sera par exemple possible de fixer la clé de répartition chaque année ou de l'adapter si l'utilisation de la plateforme fluctue fortement.

²⁰ RS 173.110.132.

Art. 19 Échéance

Al. 1

La corporation de droit public percevra l'émolument chaque année. L'émolument est dû le 1^{er} janvier, ce qui garantit que la corporation disposera des liquidités nécessaires.

Al. 2

La disposition prévoit une règle spécifique pour la première année d'exploitation : l'émolument sera dû le jour de l'entrée en vigueur de l'ordonnance. Cette règle permet d'éviter une impasse financière au cas où la date d'entrée en vigueur ne coïnciderait pas avec le 1^{er} janvier.

Art. 20 Service comptable cantonal

Chaque canton désigne un service comptable responsable afin de faciliter la facturation et les paiements à la corporation de droit public.

Art. 21 Évaluation des règles de calcul de l'émolument

Vu la marge de manœuvre étendue que le législateur a conférée au Conseil fédéral pour fixer le montant de l'émolument, il est indiqué de soumettre le calcul à un examen après un certain délai. L'examen visera à déterminer si les règles établies sont encore pertinentes et cohérentes et permettent d'assurer la stabilité financière lorsque la plateforme sera en pleine exploitation. Le DFJP sera chargé de mener l'évaluation deux ans après que l'utilisation de la plateforme centralisée sera devenue obligatoire, pour la Confédération et les cantons, dans les procédures auxquelles s'applique la LPCJ. Le DFJP garantit ainsi que l'évaluation reposera sur des données réelles. Le surveillant des prix participera également à l'évaluation.

Chapitre 2 Numérisation de documents physiques

Art. 22

Les bases légales sur la numérisation des documents physiques découlent des lois de procédures applicables, en relation avec l'art. 29 LPCJ. S'agissant du Tribunal administratif fédéral, la base légale ne découle pas directement de la PA, mais de l'art. 37a de la loi du 17 juin 2005 sur le Tribunal administratif fédéral²¹.

²¹ RS 173.32

Al. 1 et 2

Les tribunaux et les autres autorités sont tenus de convertir les documents physiques qui leur parviennent en documents PDF/A. Ces documents devront de plus être convertis par un outil de reconnaissance optique de caractères (*optical character recognition* [OCR]) en documents modifiables et indexables : l'écriture manuscrite ou imprimée est transformée par l'OCR en données lisibles par la machine. L'OCR permet de travailler plus efficacement en facilitant la fonction de recherche ainsi que la sauvegarde et le traitement des documents numériques. La fonction de recherche ne devra pas être précise à 100 %, mais elle devra être automatisée au mieux. La reconnaissance optique de caractère d'un document manuscrit (par ex. d'un testament) risque d'être très imprécise en fonction de la calligraphie.

Les documents numérisés selon cette disposition constituent la version qui fait foi dans la procédure (voir l'art. 29, al. 3, LPCJ).

Les documents numérisés devront présenter une profondeur de couleur d'au moins 8 bits (ce qui correspond à 256 nuances de gris et de couleurs) et une résolution de 300 DPI, afin de garantir clarté et lisibilité. Il faudra prévoir au besoin des valeurs plus élevées (par ex. 24 bits de profondeur de couleur ou 600 DPI), notamment pour des originaux en couleur ou très détaillés. Ces normes de qualité minimales garantissent que les documents resteront nets même en cas d'agrandissement ou d'impression.

Al. 3

Les autorités devront assurer un contrôle de la qualité approprié pour garantir que les documents numérisés correspondent bien aux originaux, et ce quant à leur aspect visuel (par ex. mise en page, images) et quant à leur contenu (par ex. précision du texte). Ce contrôle vise aussi à éviter des erreurs, comme des pages manquantes, des passages illisibles ou des images déformées. La version numérique doit être entièrement équivalente à l'original. Cela implique en pratique l'introduction de processus comme les contrôles manuels par échantillonnage, la validation automatique ou la certification. Les autorités seront libres de choisir la procédure de contrôle de la qualité qui leur convient.

Chapitre 3 Transmission de documents par un autre moyen qu'une plateforme au sens de la LPCJ

Section 1 Recours à d'autres solutions pour la transmission de documents

Art. 23 Exigences

Conformément aux lois de procédure applicables, les documents peuvent également être transmis par d'autres moyens qu'une plateforme au sens de la LPCJ. Dans ce cas, les conditions énumérées ci-après devront être remplies.

Lettre a

L'heure de transmission devra être enregistrée de manière adaptée. L'ordonnance ne prescrit pas comment il faut procéder sur le plan technique. Le système pourra délivrer des quittances séparées, recourir à un fichier journal ou à un journal d'audit (ou piste d'audit). Ce qui est important, c'est que l'heure enregistrée ne puisse pas être modifiée (ultérieurement) sans que la modification soit visible.

Lettre b

Il faudra également garantir que l'heure enregistrée soit synchronisée avec l'heure officielle suisse. Des écarts minimes jusqu'à une minute seront admissibles. Même si une différence d'une minute peut sembler longue, de tels retards peuvent résulter d'une surcharge du système.

Lettre c

Cette disposition vise à garantir que les pièces de dossier transmises par un autre moyen qu'une plateforme ne seront pas seulement protégées contre la prise de connaissance et la modification non autorisées à leur destination, mais pendant toute la transmission.

Art. 24 Transmission par voie électronique entre les autorités

Des documents peuvent aussi être transmis entre les autorités, y compris les tribunaux et services officiels au sens de l'art. 128c, al. 2, CPC, par un autre moyen qu'une plateforme au sens de la LPCJ. Celle-ci définit la communication électronique comme une procédure traçable pour toutes les parties, qui aboutit lors de tout acte pertinent à la délivrance d'une quittance contenant un cachet électronique réglementé. Cette traçabilité ne doit pas être éludée par les exceptions prévues dans les lois de procédure.

La traçabilité doit aussi être garantie par l'enregistrement, non modifiable, du nom, de la taille et de la valeur de hachage des documents transmis et de l'heure.

Distinction à faire par rapport à la consultation de bases de données

L'autorité compétente examine également si l'activité prévue constitue réellement une transmission de documents au sens de la LPCJ. Tel n'est pas le cas lors de l'interrogation d'une base de données appartenant à une autre autorité. On peut penser à la consultation du système MACS (Multiple Applications Coordination Services) lors de contrôles d'identité ou du système d'information relatif à l'admission à la circulation lors de contrôles de véhicules. Dans ces deux cas, la police consulte directement les bases de données.

Section 2 Transmission de documents par voie électronique dans le domaine de la poursuite pour dettes et la faillite

Art. 25

Dans le domaine de la poursuite pour dettes et la faillite, le réseau d'échange de données « e-LP » (LP électronique) qui utilise la plateforme sedex, est désormais bien établi. Sedex est une plateforme sécurisée pour l'échange électronique de données en Suisse, qui est exploitée et surveillée par la Confédération. Elle est utilisée dans le cadre du projet « e-LP », qui permet aux créanciers, débiteurs et offices des poursuites d'échanger de manière automatisée et chiffrée des informations et des documents de poursuite, comme des commandements de payer, des procès-verbaux de saisie ou des réquisitions de vente. En 2024, un total de 2 598 112 poursuites et 878 919 extraits de registre ont été transmis via e-LP/sedex.

La disposition actuelle concernant « e-LP » figurait dans l'OCEI-PCPP. Le contenu de la disposition sera transféré à l'art. 33b LP lors de l'entrée en vigueur de la LPCJ. Il suffit donc de prévoir dans l'AP-OCEP une règle de délégation au DFJP. L'ordonnance du DFJP du 9 février 2011 concernant la communication électronique dans le domaine des poursuites²² se fondera ainsi toujours sur une base légale suffisante.

La terminologie utilisée à l'al. 2 est spécifique au réseau « eLP ». Le terme de « boîte postale électronique » ne constitue pas une boîte de courrier électronique, mais un service de notification et de réception juridiquement contraignant.

Section 3 Attestation par voie électronique de l'exactitude du procès-verbal en procédure pénale et en procédure pénale militaire

Art. 26

Al. 1

Les parties qui confirment l'exactitude du procès-verbal devront apposer l'attestation en personne et manuellement, sans l'intervention de tiers ou de processus automatiques. Cette exigence empêche qu'une attestation puisse être copiée ou falsifiée et garantit la présence physique de la personne concernée.

Al. 2

En plus de l'heure exacte de l'attestation, les détails biométriques, notamment les caractéristiques du trait (par ex. épaisseur et forme), la pression, le flux du mouvement (par ex. vitesse) et la direction du mouvement devront être enregistrés. Ces données devront être reliées à l'attestation. C'est la traçabilité, pertinente en termes de

²² RS 281.112.1

preuves, qui importe : ces données rendent l'attestation unique et vérifiable, de manière comparable à une analyse graphologique de l'écriture manuscrite.

Al. 3

Le support électronique utilisé pour enregistrer l'attestation devra être configuré de manière à ce que le procès-verbal ne puisse plus être modifié après la première attestation de sa conformité – à l'exception de l'ajout d'autres attestations (par ex. d'autres participants), pour garantir l'intégrité du procès-verbal et empêcher toute manipulation ou falsification.

Al. 4

Cette disposition précise que la conformité d'un procès-verbal qui doit être signé uniquement par des membres d'autorités pourra aussi être attestée par voie électronique. Concrètement, les cachets électroniques réglementés et les signatures électroniques qualifiées sont équivalents aux attestations électroniques apposées sur un support électronique au sens des lois de procédure applicables.

Chapitre 4 Dispositions finales

Art. 27 Abrogation et modification d'autres actes

L'annexe 1 mentionne les deux actes à abroger et l'acte à modifier à l'entrée en vigueur de l'ordonnance.

Art. 28 Entrée en vigueur

Cette disposition contient la date d'entrée en vigueur de l'ordonnance.

4 Commentaire de l'annexe (abrogation et modification d'autres actes)

4.1 Abrogation de l'ordonnance du 18 juin 2010 sur la communication électronique dans le cadre de procédures administratives (OCEI-PA)²³

La base légale de l'OCEI-PA se trouve dans les dispositions de la PA sur la transmission électronique qui sont actuellement en vigueur. Ces dispositions seront supprimées lorsque l'ensemble de la LPCJ entrera en vigueur et seront remplacées par de nouvelles dispositions. L'OCEI-PA doit être abrogée faute de base légale.

²³ RS 172.021.2

4.2 Abrogation de l'ordonnance du 18 juin 2010 sur la communication électronique dans le cadre de procédures civiles et pénales et de procédures en matière de poursuite pour dettes et de faillite (OCEI-PCPP)²⁴

Voir les explications données au ch. 4.1.

4.3 Ordonnance du 23 novembre 2016 sur la signature électronique²⁵

Art. 14a Signatures et cachets électroniques vérifiés par le validateur

Al. 1

Cette disposition limite l'obligation de vérification du validateur aux signatures électroniques qualifiées, aux cachets électroniques réglementés et à l'horodatage électronique qualifié, car seules ces signatures produisent des effets juridiques. De plus, le validateur peut vérifier d'autres signatures électroniques s'il l'estime judicieux, par exemple les certificats de classe B de l'administration fédérale.

Al. 2

Le 29 janvier 2025, le Conseil fédéral a chargé le DETEC (OFCOM) d'élaborer, en collaboration avec le DFAE, un mandat de négociation avec l'UE en vue de la reconnaissance mutuelle des signatures électroniques. Dans le cadre de ce mandat de négociation, des craintes de voir le validateur devenir l'organisme de vérification pour toute l'UE ont vu le jour. L'al. 2 prévoit qu'à défaut d'obligation spécifique de vérification des signatures électroniques reconnues réciproquement dans les accords internationaux concernés, le validateur vérifie uniquement les signatures selon le droit suisse.

Al. 3

Pour les documents qui contiennent plusieurs signatures ou cachets, le validateur doit indiquer clairement lesquels remplissent les prescriptions de la SCSE ou d'un accord international. En lieu et place d'une évaluation générale, l'utilisateur (par exemple, une autorité) recevra des informations spécifiques indiquant les éléments qui sont valables et ceux qui ne le sont pas. Ce mode de procéder facilite le traitement des documents complexes, comme les contrats conclus entre plusieurs parties, contribue à prévenir les malentendus et aide à décider si un document peut être accepté dans son intégralité. Le validateur ne donne toutefois aucune information sur les types d'effets juridiques déployés par le document vérifié.

²⁴ RS 272.1

²⁵ RS 943.032

Al. 4

Lorsqu'un cachet d'une autorité est utilisé, le validateur peut indiquer qu'il s'agit d'un document émanant d'une autorité et préciser dans quel but le document a été créé. Il peut par exemple indiquer qu'il s'agit d'une communication officielle, de documents de la plateforme de publication de la Confédération ou d'un extrait du casier judiciaire. Cette fonction du validateur facilitera le classement des documents vérifiés et pourra contribuer à une meilleure efficacité.

Art. 14b *Processus de validation*

L'expérience a montré que l'un des principaux problèmes rencontrés en matière de validation des signatures électroniques résidait dans la marge de manœuvre importante laissée par les normes techniques internationales. Cette liberté est source de problèmes, car il n'est pas possible de tenir compte de chaque possibilité de mise en œuvre. Cette disposition a pour but de permettre à l'OFCOM de régler clairement le processus de validation et ainsi de promouvoir l'uniformisation des normes pour assurer des validations fiables et reproductibles. Cette disposition potestative ne doit toutefois pas être comprise comme l'attribution à l'OFCOM du mandat de régler le processus de validation.

Si l'élaboration par l'OFCOM de règles sur le processus de validation devait s'avérer nécessaire, l'office devra tenir compte des normes internationales et apporter des précisions uniquement dans les cas où les prescriptions internationales ne sont pas suffisamment claires.

5 Commentaire de l'art. 26, al. 5, LPCJ

L'art. 26, al. 5, LPCJ a été ajouté au cours des débats parlementaires et n'est pas mentionné dans le message. Lors des délibérations parlementaires, le Conseil fédéral a proposé de commenter la disposition ultérieurement, ce qui explique l'ajout du présent chapitre.

L'al. 5 découle de la volonté d'instaurer, en plus de la possibilité offerte par l'art. 26, al. 1, LPCJ, un moyen supplémentaire de respecter les délais en cas d'impossibilité d'accéder à la plateforme. En effet, l'art. 26, al. 1, LPCJ ne permet pas de couvrir l'ensemble des cas de figure envisageables, par exemple celui de l'absence, prévisible, de l'utilisateur pour cause de vacances, qui ne peut pas attendre que la plateforme soit à nouveau accessible.

C'est pourquoi l'art. 26, al. 5, LPCJ prévoit que le délai est également réputé respecté lorsque l'utilisateur a remis tous les documents sur papier à La Poste ou à une représentation diplomatique ou consulaire suisse.

Si les documents et leurs annexes sont volumineux, il peut s'avérer impossible de les déposer dans une boîte aux lettres après la fermeture de La Poste, raison pour laquelle l'art. 26, al. 5, LPCJ prévoit que le délai est également respecté dans les cas

où l'utilisateur se limite à apporter la preuve de l'existence des documents à remettre. La somme de hachage des documents qui sont joints au courrier peut notamment être mentionnée, de manière comparable à ce qui est indiqué dans les quittances de réception. Cela ne libère toutefois pas l'expéditeur de l'obligation de déposer les documents dans les délais dans une boîte aux lettres ou de les remettre à une représentation diplomatique ou consulaire suisse. Il convient en outre de veiller à utiliser un algorithme de hachage sécurisé, par exemple SHA-256, SHA-512, SHA-3, BLAKE2 ou BLAKE3. Les algorithmes obsolètes, comme MD5 ou SHA-1, ne doivent pas être utilisés, car ils ne sont plus sûrs.

6 Conséquences

6.1 Conséquences pour la Confédération

Sur le plan du personnel, l'ordonnance n'aura pas de conséquences allant au-delà du besoin de ressources déjà exposé au ch. 6.1 du message concernant la LPCJ. Sur le plan des finances, le message a déjà précisé que les frais d'exploitation et de développement de la plateforme seraient financés par le prélèvement d'émoluments, et que ces coûts pourraient être largement compensés par des économies à moyen ou long terme.

De plus, les unités administratives de la Confédération devront ouvrir un compte tant sur la plateforme centralisée que sur la plateforme pour les procédures administratives, et devront consulter ces comptes régulièrement, à moins qu'ils y accèdent par une interface.

6.2 Conséquences pour les cantons et les communes

Les explications qui figurent au ch. 6.1 valent également pour les cantons et les communes, sous réserve du fait que seuls les tribunaux, les ministères publics et les autorités de police devront disposer d'un compte sur la plateforme centralisée dès l'entrée en vigueur. Au besoin, les autres autorités cantonales pourront rejoindre la plateforme ultérieurement, lorsqu'ils devront communiquer pour la première fois avec les tribunaux, les ministères publics, les autorités de police ou d'autres unités administratives de la Confédération.

Les cantons devront en outre adapter leurs bases légales au besoin, si leurs actes renvoient à l'OCEI-PA ou à l'OCEI-PCPP, vu que ces ordonnances seront abrogées à l'entrée en vigueur de l'ordonnance.

6.3 Conséquences économiques

La numérisation progresse et un nombre croissant de démarches peuvent être menées en ligne. Comme le Conseil fédéral l'avait déjà souligné lors de l'élaboration du CPC, une justice efficace contribue à la prospérité économique et, en fin de compte, à l'amélioration de la qualité de vie.

La réglementation et la sécurité des échanges dans le cyberspace améliorent l'attrait et la compétitivité de la place économique suisse. Le Conseil fédéral entend faire

en sorte que l'État contribue autant que nécessaire au passage réussi de la Suisse à une société de l'information. Dans ce but, il a pris de nombreuses mesures visant principalement à adapter le cadre légal ou des éléments d'infrastructure (par ex. la SCSE ou la création de numéros d'identification uniques pour les personnes et les entreprises et des registres correspondants). Avec la LPCJ, il franchit une étape supplémentaire en soumettant les autorités et les professionnels du droit à l'obligation de recourir à la communication électronique. Pour ce faire, il prévoit la création d'une plateforme centralisée sûre et facile à utiliser, dont le fonctionnement devrait aussi séduire les personnes et les entreprises non soumises à l'obligation. Cette plateforme permettra le traitement électronique des procédures de bout en bout, pour une justice plus efficace.

Les avocats sont concernés au premier chef. Ils ne pourront plus à l'avenir déposer des actes de procédure et des pièces jointes auprès des tribunaux et des autorités (de poursuite pénale) sur papier, mais devront le faire par voie électronique. Cette nouveauté modifie le mode de travail, mais n'entraîne pas impérativement des coûts supplémentaires. Ceux-ci peuvent découler de l'adaptation de l'infrastructure, d'un besoin de personnel supplémentaire ou d'une augmentation du temps nécessaire pour effectuer certaines tâches.

6.4 Conséquences sociales

L'ordonnance aura peu de conséquences directes pour la société.

Elle ne changera rien à la manière de communiquer avec la justice pour les personnes qui ne seront pas soumises à l'obligation d'utiliser une plateforme de communication électronique. Celles-ci pourront continuer de communiquer avec les autorités par voie postale. La nouveauté, c'est qu'elles pourront également bénéficier des avantages du nouveau système qui permet une communication simple et sûre par la voie électronique. Mais chaque personne pourra décider pour elle. Pour pouvoir bénéficier de la communication électronique dans le domaine judiciaire, il faut seulement disposer d'une connexion à Internet, d'un compte sur la plateforme centralisée ou sur la plateforme pour les procédures administratives ainsi que d'un identifiant AGOV.

Quant aux professionnels du droit, ils seront soumis aux mêmes conditions.

7 Aspects juridiques

7.1 Sécurité de l'information

L'utilisation abusive d'informations et la perturbation de la plateforme centralisée sont susceptibles de porter une atteinte considérable aux intérêts essentiels de la Suisse ainsi qu'aux droits individuels. Elles risquent en outre de compromettre les tâches légales liées à l'exploitation de la plateforme centralisée et de la plateforme pour les procédures administratives. À cet égard, la LSI et l'ordonnance du 8 novembre 2023

sur la sécurité de l'information (OSI)²⁶ constituent les bases qui permettent d'assurer au mieux la sécurité de l'information.

Il n'est pas nécessaire de prévoir dans l'avant-projet des règles particulièrement détaillées concernant la manière d'aborder les menaces en matière de sécurité de l'information, puisque la LSI et l'OSI offrent déjà les bases légales nécessaires au traitement de ces menaces. Comme pour la LPD, l'on renvoie sur ce point également à la systématique actuelle du droit ; en d'autres termes, les dispositions du droit en vigueur sont suffisantes pour assurer la gestion des risques potentiels en matière de sécurité de l'information.

7.2 Protection des données

La LPD et les ordonnances y relatives s'appliqueront à la plateforme centralisée et à la plateforme pour les procédures administratives. S'agissant des procédures en cours, le droit de procédure applicable régit les traitements de données personnelles et les droits des personnes concernées (art. 2, al. 3, LPD). Afin d'éviter les répétitions et de faciliter l'interprétation des normes, l'avant-projet ne renvoie pas aux dispositions pertinentes de la LPD. Il se concentre sur le cadre créé dans la LPCJ pour le traitement, la conservation et l'effacement des données.

²⁶ RS 128.1