RÉPUBLIQUE ET CANTON DE GENÈVE

POST TENEBRAS LUX

Genève, le 1er juillet 2026

Le Conseil d'Etat

2854-2026

Département fédéral de justice et police
Monsieur Beat Jans
Conseiller fédéral
Palais Fédéral Ouest
3003 Berne

Concerne : consultation fédérale relative au projet d'ordonnance sur la communication électronique dans les procédures judiciaires et administratives régies par le droit fédéral (OCEP)

Monsieur le Conseiller fédéral,

Notre Conseil a bien reçu votre courrier du 13 mars 2026, par lequel vous avez invité les Gouvernements cantonaux à se prononcer dans le cadre de la procédure de consultation citée en marge.

Après en avoir pris connaissance avec intérêt et attention, nous vous prions de trouver, dans le document annexé à la présente, la prise de position du Conseil d'État, établie en concertation avec le Pouvoir judiciaire.

En vous remerciant de nous avoir consultés, nous vous prions de croire, Monsieur le Conseiller fédéral, à l'assurance de notre haute considération .

AU NOM DU CONSEIL D'ÉTAT

La chancelière :

Michèle Righetti-El Zayadi

La présidente :

Anne Hiltpold

Annexe mentionnée

Copie à (*format Word et pdf*) : cornelia.perler@bj.admin.ch

Annexe

Consultation fédérale relative à l'Ordonnance sur la communication électronique dans les procédures judiciaires et administratives régies par le droit fédéral (OCEP)

Prise de position du Conseil d'État de la République et canton de Genève

---

I. Introduction

Le Conseil d'État attire en particulier votre attention sur ses observations en lien avec les articles 23 et 24 du projet, résumées ici en préambule.

- Les autorités judiciaires et les gouvernements cantonaux sont intervenus, durant les travaux parlementaires portant sur la loi fédérale sur les plateformes de communication électronique dans le domaine judiciaire (LPCJ) du 20 décembre 2024, pour que soit prévue la possibilité, pour les autorités chargées de diriger la procédure, de communiquer, dans certains cas, sous forme électronique mais sans recourir à l'une des plateformes au sens de la loi. Il s'agissait d'éviter que les autorités judiciaires ne doivent utiliser une plateforme lorsqu'elles communiquent à une autre autorité des documents ou instructions sans que ladite communication n'ait d'effet pour les parties à la procédure. Étaient notamment visées : la transmission du dossier judiciaire d'un tribunal de première instance au tribunal cantonal, la transmission du rapport de police au ministère public, la communication d'instructions du ministère public à la police ou encore la communication de documents d'une autorité administrative ou d'un service administratif à l'autorité judiciaire.

  Le Parlement fédéral a fait droit à cette demande et introduit la possibilité pour les autorités judiciaires de procéder à des communications électroniques sans recourir à la plateforme, sur un plan intracantonal (procédures civiles et pénales) et sur un plan intercantonal (procédures pénales). De telles communications électroniques doivent ainsi pouvoir intervenir sans passer par une plateforme au sens de la LPCJ, par exemple par le biais d'un interfaçage des systèmes d'information à l'intérieur d'un canton (notamment entre la police et le ministère public) ou encore par la modification ponctuelle des droits d'accès dans un système d'information commun (par exemple pour communiquer un dossier du tribunal de première instance au tribunal supérieur).

  Les articles 23 et 24 du projet d'ordonnance, censés concrétiser cette possibilité introduite durant les travaux parlementaires à la demande des autorités judiciaires, doivent impérativement être revus. Leur formulation et leur articulation sont en l'état incompréhensibles, de même que leur champ d'application concret. Ils posent en outre des exigences et conditions telles qu'ils enlèvent tout intérêt au mode alternatif de communication électronique introduit dans la LPCJ.

  Au vu de la technicité de cette question, le Conseil d'État recommande que l'office fédéral de la justice remette l'ouvrage sur le métier en concertation avec le groupe d'experts du projet Justitia 4.0, notamment composé de magistrats expérimentés pouvant expliquer les enjeux en présence et apporter un éclairage indispensable.

- La plateforme justitia.swiss propose en principe la communication du document lui-même. Elle teste toutefois avec le canton de Bâle-ville une alternative avec le stockage décentralisé des documents dans les systèmes d'information de ce canton, la plateforme y donnant simplement accès. Dans cette variante, le document ne transite pas par la plateforme. Le canton de Genève pourrait être intéressé par ce mode de fonctionnement mais s'interroge sur les éléments suivants : a) la plateforme ne peut vérifier si les documents sont munis d'un cachet électronique, b) elle ne peut vérifier que les documents sont exempts de logiciel malveillant et c) elle peut émettre une quittance de consultation sans pouvoir vérifier que le document existe ou est accessible. Il paraît important que ces questions soient vérifiées et traitées pour les cantons souhaitant adopter le mode décentralisé.

- Le Conseil d'État souligne en outre l'importance des observations formulées en lien avec l'article 4, alinéa 2, ainsi qu'avec deux articles nouveaux qu'il est proposé d'introduire, soit les articles 22a et 22b.

II. Commentaires d'articles

Concernant le préambule du projet d'ordonnance

Le projet d'ordonnance omet délibérément de citer les articles qui confèrent au Conseil fédéral la compétence de réglementer le format des documents transmis par voie électronique. Le rapport explicatif précise que, « *pour conserver une vue d'ensemble* », le préambule ne mentionne que les dispositions des lois de procédure qui traitent de la communication en dehors des plateformes de la LPCJ. Le canton de Genève estime qu'il est préférable de mentionner toutes les normes de délégation contenues dans les lois de procédure. Cela vaut en particulier pour les articles qui confèrent au Conseil fédéral la compétence de définir les formats. Ces dispositions devraient donc logiquement être également mentionnées dans le préambule, qui devrait ainsi être libellé comme suit:

> *vu la loi fédérale du 20 décembre 2024 sur les plateformes de communication électronique dans le domaine judiciaire (LPCJ),*
> *vu l'art. 6a al. 2, 21a al. 2 et 34 al. 1bis de la loi du 20 décembre 1968 sur la procédure administrative du 20 décembre 1968 (PA),*
> *vu l'art. 38e de la loi sur le Tribunal fédéral du 17 juin 2005 (LTF),*
> *vu les art. 128b al. 3 et 128c al. 2 et 128e du code de procédure civile du 19 décembre 2008 (CPC),*
> *vu les art. 33a al. 4, 33b, 33c al. 2 et 34 al. 3 de la loi du 11 avril 1889 sur la poursuite pour dettes et la faillite (LP),*
> *vu les art. 76a al. 2, 103b al. 3, et 103c al. 2 et 103e du code de procédure pénale du 5 octobre 2007 (CPP),*
> *vu l'art. 2e de la loi fédérale du 23 décembre 2011 sur la protection extraprocédurale des témoins (Ltém),*
> *vu l'art. 31f de la loi fédérale du 22 mars 1974 sur le droit pénal administratif (DPA),*
> *vu les art. 8c al. 3, et 8d al. 2 et 8f de la loi du 23 mars 2007 sur l'aide aux victimes (LAVI),*
> *vu les art. 37d et 38a al. 2 de la procédure pénale militaire du 23 mars 1979 (PPM),*

Ad article 1

Selon notre interprétation, l'alinéa 2 concerne exclusivement les procédures qui, en vertu de la loi sur la procédure administrative (PA), relèvent du droit fédéral, étant rappelé que les procédures administratives cantonales sont exclues du champ d'application de la LPCJ.

L'alinéa 3 peut être supprimé.

Ad article 2 Conditions applicables aux plateformes

Compte tenu de l'évolution rapide des technologies, la taille maximale des fichiers visée à l'alinéa 1, lettre c, doit être fixée dans une annexe à l'ordonnance soumise à la présente consultation, ou dans une ordonnance du département fédéral de justice et police. Le Conseil d'État considère en effet que l'OCEP n'est pas le bon niveau normatif pour régler cette question. Elle doit en revanche contenir une norme de délégation sur ce point.

La lettre d de l'alinéa premier de cette disposition n'a pas sa place à cet endroit. Elle définit en effet une fonctionnalité, qui doit être réglementée dans la section 3 de l'ordonnance. Par ailleurs, la formulation est trop absolue et difficilement applicable. Comme le souligne à juste titre le rapport explicatif, à la page 11, la fonction de suppression a pour effet d'effacer l'autorisation individuelle accordée mais pas le document lui-même. Il convient en outre, s'agissant de la fonction de suppression, de faire la distinction entre les autorités et les autres utilisateurs.

Ad article 4 **Format des documents**

Remarque générale

Le projet utilise, à l'instar de la LPCJ, le terme « document » plutôt que celui de « fichier » (cf. message LPCJ, p. 20), au motif que le terme « fichier » est un terme trop technique pour être utilisé dans la loi. Le terme « fichier » doit en revanche être utilisé dans l'ordonnance, qui qualifie d'un point de vue technique les annexes transmises.

Ad alinéa 2

Le Conseil d'État souligne que l'alinéa 2 de l'article 4 doit impérativement être modifié.

En effet, dans la très grande majorité des cas, le format PDF suffit pour reproduire le contenu informatif d'un document de manière juridiquement valable. Pour ce motif, les pièces doivent être déposées dans ce format largement répandu. Cela facilite le traitement des dossiers par les avocates et avocats, les ministères publics, les tribunaux, les autorités administratives et les autres parties à la procédure. En soumettant leurs pièces jointes en format PDF, les parties évitent leur conversion par les autorités judiciaires en format PDF et toutes les parties disposent du même document.

La numérisation vise à accélérer les procédures et à simplifier la gestion des dossiers. Si en règle générale les documents sont disponibles au format PDF, cela permettra un traitement rapide par les avocates et avocats et les autorités. Pour des raisons de sécurité, les systèmes de gestion des dossiers des avocates et avocats et des autorités ne peuvent traiter qu'un nombre limité de types de fichiers (« White-listening » des formats de fichiers). Si le format des pièces jointes pouvait être choisi librement, cela compliquerait considérablement le traitement des dossiers. Toutes les parties à la procédure devraient d'abord rechercher le programme approprié pour ouvrir un fichier. Elles devraient en outre le convertir pour pouvoir utiliser pleinement les applications permettant de travailler avec un dossier judiciaire électronique. Les avocates et avocats ou les autorités administratives devraient faire de même. Il en découlerait un surcroît de travail important et, partant, une perte d'efficience, sans pour autant qu'il n'y ait de valeur ajoutée au dépôt du document sous un autre format. Il en découlerait en outre des risques de confusion.

En d'autres termes, il est important de prévoir que les parties et les avocates et avocats doivent en principe produire les annexes en fichier PDF et non en format original. Dans la quasi-totalité des cas, la production du fichier original (par exemple Excel, Word ou PowerPoint) ne présenterait aucune valeur ajoutée et entraverait l'utilisation des applications de travail avec les dossiers judiciaires électroniques. Dans les rares cas où la partie ou l'avocate ou l'avocat estime que le fichier original doit être produit au motif qu'il contient des informations importantes que le fichier PDF ne contiendrait pas, la production du fichier original doit évidemment être possible.

À noter par ailleurs que le choix illimité des formats constituerait un risque considérable pour la sécurité informatique de toutes les parties concernées.

Pour le surplus, même avec une liste élargie de formats acceptables, certains fichiers ne pourront être lus, en raison d'un format moins courant. On peut notamment penser à des enregistrements audio ou vidéo.

Pour des raisons de sécurité, la plateforme analyse tous les fichiers pour détecter des virus. Ce faisant, la plateforme ne peut en principe analyser de manière efficace que les formats de fichiers qu'elle connaît. Pour les documents qui ne peuvent pas être transmis directement via la plateforme, il est possible de les transmettre dans un conteneur, par exemple au format ZIP.

Enfin, les formats de fichiers que la plateforme doit prendre en charge doivent être définis par le DFJP dans une ordonnance départementale, après consultation de l'exploitant de la plateforme centrale.

Au vu de ce qui précède, le Conseil d'État considère que l'alinéa 2 devrait être libellé comme suit :

> [2] ~~*Les annexes peuvent être remises dans n'importe quel format*~~ *Si le format PDF ne permet pas de restituer correctement le contenu d'un document, l'annexe peut être transmise dans son format d'origine*.

Ad alinéas 3 et 4

Si la sélection de formats de fichiers proposée peut convenir, le niveau normatif est inadéquat. La définition des formats que les autorités chargées de la procédure doivent pouvoir traiter devrait figurer dans une annexe à l'OCEP ou dans une ordonnance départementale du DFJP.

La liste des formats de fichiers pris en charge est en constante évolution. Il faut donc s'attendre à des adaptations fréquentes. De plus, la simple mention des formats de documents dans l'ordonnance n'est pas suffisante. D'autres détails techniques, tels que le traitement des fichiers protégés par mot de passe ou cryptés, doivent être réglementés, y compris, le cas échéant, les éléments individuels d'un fichier ouvert qui sont néanmoins cryptés ou protégés par mot de passe (par exemple, les macros dans un fichier Microsoft Excel, les fichiers ZIP contenant des fichiers partiellement cryptés, etc.).

Ces éléments doivent figurer dans une annexe à l'ordonnance.

Les alinéas 3 et 4 devraient donc être libellés comme suit :

> [3] ~~*L'autorité qui dirige la procédure doit pouvoir traiter les formats suivants :*~~*Si l'autorité qui dirige la procédure ne peut ouvrir une pièce jointe dans le format dans lequel elle a été transmise, elle accorde à la partie qui l'a transmise un délai approprié pour la transmettre dans un format défini par l'autorité.*
> ~~*a. documents écrits : PDF, PDF/A ;*~~
> ~~*b. images : BMP, GIF, JPEG, PNG ;*~~
> ~~*c. fichiers audio : MP3, OGG, WAV ;*~~
> ~~*d. fichiers vidéo : AVI, MOV, MKV, MP4 ;*~~
> ~~*e. fichiers d'archives : ZIP, 7z.*~~
> [4] ~~*Lorsqu'une annexe a été remise dans un autre format et que l'autorité qui dirige la procédure ne peut pas la traiter de manière appropriée, l'autorité demande à la personne ou à l'autorité qui a remis l'annexe de la renvoyer dans un format déterminé ou d'y donner accès de façon adaptée*~~ *Le DFJP définit les formats de fichiers à transmettre via la plateforme*.
> [5] ~~*L'autorité qui dirige la procédure fixe un délai approprié.*~~

Ad article 5 **Quittances**

Le nom de la personne responsable d'une autorité, au sens de **l'alinéa 2, lettre b**, ne doit pas figurer sur la quittance. Seul le nom de l'autorité doit apparaître.

Un résultat positif lors du contrôle antivirus visé à **l'alinéa 2, lettre d, chiffre 2**, constitue un motif possible de rejet du fichier par la plateforme, mais ce n'est pas le seul. La taille ou le format du fichier peuvent également en être la cause. Nous sommes d'avis que la quittance doit pouvoir faire mention des autres causes de rejet.

L'alinéa 2, lettre d, chiffre 2, précise que les documents qui n'ont pas été transmis suite au résultat de l'analyse de l'antivirus sont mentionnés dans la quittance de réception. Nous considérons que la quittance devrait le cas échéant faire également mention de la valeur de hachage des documents rejetés, pour éviter tout contentieux ultérieur sur la nature du document dont la transmission a échoué. Le chiffre 2 devrait être modifié en conséquence :

> [2] *Les quittances comportent en particulier les données suivantes:*
> *a. le type de quittance ;*
> *b. le nom de l'expéditeur, son adresse sur la plateforme et le cas échéant le nom de l'organisation ou de l'entreprise pour laquelle il agit;*
> *c. le nom du destinataire ou de son entreprise et son adresse sur la plateforme;*
> *d. pour la quittance de réception :*
> *1. la liste des documents transmis, leur taille et leur valeur de hachage,*
> *2. la liste des documents qui n'ont pas été transmis, avec indication de leur taille, de leur valeur de hachage et de la raison de la non-transmission,*
> *3. le moment de la transmission à la plateforme ;*

À noter qu'il existe plusieurs algorithmes permettant de calculer la valeur de hachage. Afin de garantir la traçabilité et la validité juridique de cette valeur, l'algorithme utilisé pour son calcul doit être explicitement identifié. Il est proposé d'intégrer une clause de délégation permettant au département de définir et de publier l'algorithme applicable pour le calcul des valeurs de hachage.

Les plateformes permettront à l'avenir de transmettre des données structurées, par exemple sous forme de fichiers XML. Les exceptions prévues aux alinéas 4 et 5 sont donc essentielles, car pour des raisons techniques, les fichiers XML ne peuvent ou ne doivent pas forcément être cachetés.

Ad article 6 **Apposition d'un cachet par l'autorité expéditrice**

Dans le cadre de la communication électronique dans le domaine judiciaire, le cachet électronique devra désormais être apposé à deux étapes distinctes. L'autorité qui dirige la procédure apposera son cachet sur l'un des documents transmis avant leur envoi à la plateforme ; il s'agira généralement de la décision (ordonnance, jugement, arrêt) ou d'une correspondance. La plateforme au contraire apposera un cachet après la transmission à la plateforme, sur la quittance émise sur la base de l'article 5.

L'article 6 règle l'apposition d'un cachet sur les documents par l'autorité dirigeant la procédure avant leur transmission par l'intermédiaire d'une plateforme (art. 22 al. 2 LPCJ). Le projet prévoit que « *lorsqu'une autorité transmet à la plateforme plusieurs documents en même temps, il suffit qu'un de ces documents soit muni d'un cachet et d'un horodatage* », ce qui est correct. On ajoutera que l'apposition d'un cachet par l'autorité qui dirige la procédure a lieu indépendamment du nombre de documents transmis. Même si un seul document est transmis par l'autorité qui dirige la procédure, celui-ci doit être muni d'un cachet, afin que l'authenticité du document puisse être examinée indépendamment de la plateforme.

Les explications figurant dans le rapport explicatif, selon lesquelles une autorité doit apposer un cachet électronique sur tous les documents, contredisent le libellé de l'ordonnance. L'apposition d'un cachet sur un seul document par l'autorité qui dirige la procédure suffit et doit impérativement suffire. Par ailleurs, l'obligation faite aux autorités qui dirigent la procédure et aux autorités qui y participent d'apposer un cachet est en contradiction avec le concept technique de la plateforme centralisée.

Pour diverses fonctionnalités de la plateforme centrale, la distinction entre les autorités qui dirigent la procédure et les autorités participant à la procédure est essentielle. Ainsi, seules les autorités qui dirigent la procédure pourront procéder à des notifications. Seules les adresses des autorités qui dirigent la procédure seront visibles pour les tiers dans le répertoire public de la plateforme. Si l'obligation d'apposer un cachet était maintenue pour les autorités participant à la procédure ou communiquant avec l'autorité qui dirige la procédure, toutes les autorités pourraient effectuer sans restriction des notifications à d'autres autorités, organisations, avocats et particuliers et ce, indépendamment d'une procédure contentieuse. Cela étendrait l'utilisation de la plateforme à toute communication électronique entre autorités, sans aucune base légale. Pour mémoire, l'objectif de la LPCJ est de permettre la communication électronique dans le cadre des procédures judiciaires.

Seules les autorités qui dirigent la procédure sont tenues d'apposer un cachet électronique sur leurs documents. L'article 22, alinéa 2, LPCJ doit donc être interprété de manière restrictive. Le cachet électronique garantit l'origine, la date exacte, l'intégrité et l'authenticité du document muni d'un cachet. La décision incidente ou le jugement d'une autorité qui dirige la procédure crée des droits et des obligations. Les personnes concernées doivent donc pouvoir vérifier, indépendamment d'une procédure concrète ou de la plateforme centrale, si le document concerné est intègre et authentique et s'il a été établi par l'autorité compétente. En résumé, le cachet électronique est nécessaire précisément là où les autorités chargées de la direction de la procédure exercent leurs prérogatives.

Les autorités participant à la procédure ne doivent pas être tenues d'apposer un cachet électronique sur leurs documents. Les documents que les autorités parties à la procédure transmettent dans le cadre d'une procédure judiciaire ne créent pas de nouveaux droits et obligations. Il s'agit généralement d'extraits de registres existants, d'extraits de dossiers existants de procédures antérieures ou de décisions déjà notifiées issues de procédures closes, qui sont désormais mis à disposition pour une procédure judiciaire. L'authentification sur la plateforme permet l'identification correcte de l'autorité. Si une partie à la procédure souhaite contester l'intégrité ou l'authenticité d'un document transmis par une autorité partie à la procédure, il s'agit d'une question d'appréciation des preuves dans la procédure correspondante.

Si l'obligation d'apposer un cachet était maintenue pour toutes les autorités conformément au rapport, toutes les autorités suisses devraient être équipées d'un cachet à tous les niveaux. La LPCJ n'offre pas de base légale suffisante à cet effet et n'avait pas cet objectif. L'instauration généralisée d'un cachet électronique entraînerait en outre pour les cantons un effort organisationnel considérable et des coûts importants.

Selon le rapport explicatif, il n'y aurait plus lieu d'apposer un cachet sur les documents dotés d'une signature électronique qualifiée. Cette affirmation ne correspond pas au concept de la LPCJ, laquelle ne prescrit aucune fonctionnalité permettant à la plateforme de contrôler quelles signatures électroniques qualifiées sont attribuées à une autorité. C'est pourquoi les autorités dirigeant la procédure doivent également apposer un cachet sur les documents déjà munis d'une signature électronique qualifiée avant de les transmettre par l'intermédiaire de la plateforme.

Il serait utile de préciser comment les autorités peuvent signer des documents qui, selon la jurisprudence actuelle, doivent porter la signature de leur auteur, comme les expertises (BSK StPO-Heer, art. 187 N 1). Dans le cas des instituts de médecine légale ou de l'Institut fédéral de métrologie METAS, par exemple, ces expertises peuvent tout à fait être réalisées par des autorités ou, à tout le moins, par des « services administratifs ». Dans ces cas, l'identité de l'expert qui établit l'expertise

est déterminante, raison pour laquelle la signature électronique qualifiée (contrairement à ce qui ressort du commentaire de l'art. 22 LPCJ dans le message, FF 2023 679ss, p. 30) devrait probablement continuer à s'appliquer à l'avenir.

Il est important de souligner la différence entre l'envoi et consultation en ligne de documents. Comme l'explique à juste titre le rapport explicatif, il n'y a pas d'obligation pour l'autorité qui dirige la procédure d'apposer son cachet sur les documents mis à disposition pour la consultation en ligne du dossier.

Ad article 7 Apposition d'un cachet par la plateforme

Remarques générales

Dans le cadre de la communication électronique dans le domaine judiciaire, le cachet électronique devra désormais être apposé à deux étapes distinctes. L'autorité qui dirige la procédure appose son cachet sur l'un des documents transmis avant leur envoi à la plateforme ; il s'agit généralement de la décision (ordonnance, jugement ou arrêt) ou de la lettre d'accompagnement (cf. *supra* ad art. 6). La plateforme, en revanche, appose son cachet après la transmission sur la plateforme, sur la quittance de réception émise, qui est régie par l'article 5.

À noter que les conditions applicables en cas d'indisponibilité de la plateforme, notamment celles relatives à la vérification de l'intégrité des documents au moyen des valeurs de hachage, pourraient être utilement définies. L'algorithme de hachage utilisé et les modalités de contrôle et de validation pourraient être précisées, le cas échéant dans une ordonnance du département.

Ad alinéa premier

Le principe de l'apposition du cachet électronique par la plateforme a été correctement repris : le support du cachet électronique de la plateforme est la quittance, jamais le document transmis. Dans le cas de la plateforme centrale, le document distinct visé à l'article 7, alinéa 1, est la quittance de réception ou la quittance de consultation. La plateforme appose son cachet électronique sur la quittance de réception des utilisateurs, qu'ils transmettent un ou plusieurs documents. L'alinéa 1 devrait donc être libellé comme suit :

> [1] *Lorsque ~~plusieurs~~ des documents sont transmis, la plateforme appose le cachet et l'horodatage sur un document séparé. Le document mentionnera le nom, la taille et la valeur de hachage de chaque document transmis.*

Ad alinéa 2

L'alinéa 1 décrit le cachet électronique apposé sur les quittances. La transmission de documents munis d'un cachet suit les mêmes règles que celles de l'alinéa 1. L'alinéa 2 doit donc être supprimé :

> [2] *~~Les documents qui sont déjà munis d'un cachet ou d'une signature électronique qualifiée et d'un horodatage ne doivent pas être munis d'un cachet supplémentaire.~~*

Ad article 8 Authentification des utilisateurs

L'authentification par AGOV, conformément à l'alinéa 1, est judicieuse et pertinente. Le Conseil d'État est en effet favorable à une authentification simplifiée pour les collaboratrices et collaborateurs des autorités, ce qui leur permet d'éviter de passer par des étapes supplémentaires de connexion et ainsi de perdre du temps.

L'utilisation éventuelle de services d'authentification supplémentaires dans le cadre de futures plateformes cantonales, conformément à l'alinéa 2, est saluée.

À l'avenir, la plupart des autorités seront reliées à la plateforme par une interface. La disposition proposée à l'alinéa 3 laisse une marge de manœuvre suffisante pour mettre en œuvre de futures solutions techniques.

Le canton de Genève se demande par ailleurs s'il est attendu que l'authentification des membres des autorités judiciaires par leur connexion à leur application métier soit d'un niveau de qualité similaire à celui de la plateforme (AGOV aq300). Si tel était le cas, les autorités judiciaires ne seront vraisemblablement pas en mesure de le faire à bref délai.

Ad article 9 **Profils**

Remarque générale

Le canton de Genève se demande si des mesures sont prévues ou envisagées pour prévenir ou limiter les risques d'usurpation d'identité, permettant notamment la création sans contrôle de compte pour une organisation par ailleurs existante.

Ad alinéa 2

Cette disposition se réfère uniquement aux autorités chargées de la conduite de la procédure, qui figurent également dans le répertoire d'adresses de la plateforme. Dans le cas des autorités qui dirigent la procédure, il convient de renoncer à l'indication d'une adresse postale car une autorité peut disposer de plusieurs sites. La disposition doit en conséquence être adaptée comme suit :

> *[2] Les profils des autorités comprennent au moins les données suivantes :*
> *a. le nom de l'autorité ;*
> *~~b. l'adresse postale ;~~*
> *b ~~c~~. le nom du cachet.*

Ad alinéa 3, lettre a

La reprise de la date de naissance à partir du compte AGOV est particulièrement bienvenue dans le domaine du droit pénal et du droit administratif.

Il convient de souligner que l'adresse privée n'est pas mise à jour dans le compte AGOV. L'exactitude de l'adresse privée repose sur la déclaration de l'utilisateur. Elle n'est pas vérifiée lors de l'identification, ce qui la rend peu fiable. En outre, du point de vue de la protection des données, l'enregistrement de l'adresse privée dans les profils utilisateurs doit être considéré comme problématique. Il convient donc de renoncer à la collecte des adresses postales des personnes physiques et de formuler la lettre a de la manière suivante :

> *[3] Les profils des autres utilisateurs comprennent au moins les données suivantes :*
> *a. pour les personnes physiques : le prénom, le nom, la date de naissance ~~et l'adresse postale~~ ;*

Ad alinéa 3, lettre b

Les entreprises ont des structures variées et des succursales différentes, raison pour laquelle le profil numérique utilisé ne doit pas nécessairement correspondre à l'adresse postale. Cette dernière n'apporte aucune valeur ajoutée notable dans le cadre de la distribution numérique. Il convient donc de renoncer à l'adresse postale également pour les organisations.

L'alinéa 3 devrait donc être formulé comme suit :

> [3] *Les profils des autres utilisateurs comprennent au moins les données suivantes :*
> a. *pour les personnes physiques : le prénom, le nom~~,~~ et la date de naissance ~~et l'adresse postale~~ ; …*
> b. *pour les organisations : le nom de l'organisation ou de l'entreprise ~~et l'adresse postale.~~*

Ad alinéa 4

Cet alinéa n'est pas compréhensible, et il y a lieu de le clarifier. On ne comprend en effet pas s'il concerne le profil d'une organisation ou celui d'un particulier.

Le rapport mentionne la personne responsable d'une organisation. De notre point de vue, il est souhaitable que le rôle de la personne responsable sur la plateforme soit clarifié dans l'ordonnance.

Ad article 10 **Interface**

Cet article permet aux utilisatrices et utilisateurs de la plateforme de connecter leurs systèmes à celle-ci par le biais d'une interface et d'octroyer des droits de représentation à leurs collaboratrices et collaborateurs, ce qui se fait par l'intermédiaire d'un utilisateur technique, lequel reçoit un mot de passe numérique (token). La réglementation proposée est donc saluée.

Ad article 11 **Attribution et retrait de droits**

La réglementation proposée à l'alinéa 1 est adéquate et peut être mise en œuvre sur la plateforme. Dans la version française, il conviendrait cependant de parler de « confirmation » plutôt que d'« attribution ». Le titre de cette disposition deviendrait ainsi le suivant :

> *Article 11* *Confirmation et retrait de droits*

Ad article 12 **Durée maximale de conservation des documents et des quittances**

Ad alinéa premier

Problématique

L'article 12 du projet d'ordonnance prévoit que les documents et les quittances sont supprimés automatiquement de la plateforme à l'expiration d'un délai de six mois.

Le canton de Genève est favorable à la suppression automatique des documents après un délai raisonnable car la plateforme est conçue comme une « boîte aux lettres », et non comme un moyen de stockage et d'archivage. Le Conseil d'État considère cependant opportun, en ce qui concerne les quittances, de prévoir un délai un peu plus long.

Les quittances sont utiles pour prouver le respect d'un délai ou la prise de connaissance d'un document donné. Il appartient évidemment aux autorités de transférer les quittances dans leurs propres logiciels de gestion d'affaires, en les intégrant à leurs propres systèmes. Cependant, le fait qu'en raison du fonctionnement de la plateforme centralisée, les quittances ne sont pas classées dans les dossiers d'une procédure, par exemple en cas de notification, pourrait conduire à ce que le téléchargement des quittances ne soit pas effectué. Contrairement aux requêtes et aux notifications,

qui peuvent être renvoyées depuis les systèmes sources, les quittances générées par la plateforme elle-même seraient dans ce cas déjà perdues au bout de six mois.

Les quittances peuvent également contenir des données personnelles (telles que les noms des parties à la procédure), ce qui, dans le contexte des procédures judiciaires, peut même en faire des données personnelles particulièrement sensibles. Cependant, ces données, tout comme les pièces du dossier elles-mêmes, bien plus sensibles, sont stockées de manière sécurisée sur la plateforme. À cela s'ajoute le fait que les quittances constituent également de très petites quantités de données, qui ne nécessitent pas de stockage supplémentaire important, même si elles restent disponibles longtemps sur la plateforme.

Proposition

Il est proposé ici de modifier ou de retenir un délai de trois ans, qui correspond au délai pendant lequel la Poste suisse permet d'effectuer des recherches en lien avec le courrier postal.

Par ailleurs, dans la version française, le fait que la suppression est automatique manque dans le libellé de l'alinéa 1, de sorte qu'il convient de l'ajouter.

Le Conseil d'État estime que l'alinéa 1 doit donc être modifié comme suit :

Article 12 Durée maximale de conservation des documents et des quittances

[1] Les documents ~~et les quittances~~ enregistrés sur une plateforme sont automatiquement ~~détruits~~supprimés six mois après leur réception ~~ou leur délivrance~~.
[2] Lorsque des documents peuvent être consultés, l'autorité qui dirige la procédure fixe le délai pendant lequel ils sont disponibles sur la plateforme. Passé ce délai, ils sont automatiquement supprimés ~~détruits~~.
[3] Les quittances sont automatiquement supprimées trois ans après leur délivrance.

Ad alinéa 2

Le canton de Genève est favorable à la solution proposée. Il n'est pas nécessaire de prévoir une prolongation du délai dans l'ordonnance car l'autorité peut ordonner une deuxième consultation du dossier avec les mêmes pièces.

Ad article 13 Sécurité des données

La disposition proposée renvoie à la section 3; la mention du chapitre pertinent (2 ?) fait défaut et doit être ajoutée.

Il pourrait par ailleurs être ajoutée la nécessité de tenir un registre des indisponibilités des plateformes.

Par ailleurs, le canton de Genève souligne ici la problématique sécuritaire qui pourrait se poser dans le cadre de la transmission des images de vidéosurveillance. En effet, l'office cantonal de la détention en particulier est régulièrement amené à transmettre des enregistrements des images de vidéosurveillance, de ses établissements pénitentiaires aux autorités pénales ou administratives. Autoriser un accès illimité de ces images aux parties via une plateforme pourrait engendrer un problème sécuritaire, dans la mesure où celles-ci auraient la possibilité d'analyser la disposition des locaux, ainsi que l'organisation des établissements et de leurs dispositifs sécuritaires. Le canton de Genève préconise donc que, lors de la mise en place du nouveau système de communication, l'accès à ces images de vidéosurveillance soit limité.

Ad article 14 **Contrôle antivirus**

Remarque générale

Du point de vue technique, il convient de distinguer trois cas dans le cadre de l'analyse prévue visant à détecter les logiciels malveillants.

1. Analyse complète des fichiers transmis : la taille maximale de chaque fichier ne doit pas dépasser une limite supérieure définie, faute de quoi le logiciel d'analyse ne pourrait garantir l'opération pour des raisons techniques (espace de stockage, etc.) et interromprait l'analyse. Le processus d'analyse pourrait en outre prendre tellement de temps que le respect des délais serait compromis en cas d'utilisation de la plateforme quelques minutes avant l'échéance d'un délai.

2. Analyse limitée des fichiers volumineux : un fichier dépassant la taille maximale fixée est divisé en blocs inférieurs ou égaux à la taille maximale fixée, chaque bloc pouvant ainsi faire l'objet, de manière individuelle, de l'analyse de logiciels malveillants. Cette procédure est toutefois moins fiable que l'analyse complète. Les logiciels malveillants qui, du fait de la division en blocs vérifiables, sont répartis sur deux blocs consécutifs, peuvent ne plus être détectés comme logiciels malveillants. Cela doit être clairement indiqué aux utilisatrices et utilisateurs de la plateforme. Il convient notamment de signaler clairement au destinataire qu'il doit effectuer son propre contrôle complet de la présence de logiciels malveillants sur les données stockées localement après le téléchargement du fichier.

3. Renonciation au contrôle antivirus : lors de la phase pilote de la plateforme, il est apparu que les mesures de protection mises en place sont, dans certains cas, trop strictes. Les raisons suivantes (liste non exhaustive) ont été identifiées :

    - Transmission de preuves électroniques provenant d'appareils saisis, dans leur version originale ou après avoir été traitées par la police scientifique (forensique informatique), par exemple dans le cadre de la consultation du dossier.
    - Transmission de fichiers protégés par mot de passe ou chiffrés de bout en bout entre certaines autorités. Ces fichiers ne peuvent en principe pas être analysés pour permettre la détection de logiciels malveillants, car ils sont chiffrés.
    - Transmission de formats de fichiers contenant des macros ou d'autres codes exécutables. Bien qu'ils ne contiennent pas de virus au sens classique du terme, ils offrent de nombreuses possibilités d'attaque pour les cybercriminels. C'est pourquoi les formats de fichiers exécutables sont rejetés par la plateforme pilote.
    - En raison des mesures de protection, des fichiers seront rejetés à tort, bien qu'ils aient été nettoyés par les autorités expéditrices. Ce comportement est appelé « faux positifs ».

Au cours de la phase pilote, il a été demandé à plusieurs reprises de pouvoir également transmettre de tels fichiers et de ne pas avoir à recourir à des moyens de transmission alternatifs (non sécurisés) (e-mail classique, Dropbox...). Le stockage et la récupération de ces documents, y compris les éventuelles vérifications de la présence de logiciels malveillants, incombent dans ce cas aux utilisateurs de la plateforme. Si l'expéditeur et le destinataire souhaitent contourner les mesures de protection, ils réduisent la fonction de la plateforme à la simple transmission de données et sont eux-mêmes responsables de la gestion correcte des fichiers. Cela nécessite un accord entre les parties concernées. Et cela signifie également que les utilisateurs doivent effectuer leur propre analyse antivirus complète des données stockées localement, avant et après leur transmission par la plateforme. La plateforme doit en outre signaler au destinataire que les fichiers transmis dans un conteneur n'ont pas été soumis à une analyse antivirus.

Ad alinéa premier

La définition de la taille des blocs vérifiables pour les fichiers volumineux ne doit pas être communiquée publiquement. Cette information n'est pas pertinente pour les utilisateurs de la plateforme. Elle offre aux attaquants potentiels la possibilité de diffuser leurs logiciels malveillants dans un fichier infecté de telle sorte que, lors du fractionnement en blocs, le code malveillant se trouve dans deux blocs consécutifs et ne puisse pas être détecté de manière fiable comme étant nuisible. De plus, la taille de ces blocs dépendra du logiciel chargé de la division et de la vérification. Cette limite évoluera de manière dynamique en fonction de l'expérience opérationnelle et des améliorations apportées au matériel et aux logiciels. Elle doit donc pouvoir être adaptée facilement.

L'alinéa 1 devrait donc être libellé comme suit :

> [1] *Les plateformes ~~soumettent les documents ayant une taille maximale de 64 mégaoc tets~~ à effectuent un contrôle antivirus.*

Ad alinéa 2

La limite actuelle de 64 Mo pour un contrôle complet des logiciels malveillants paraît d'ores et déjà trop basse au regard des possibilités techniques actuelles. Cette limite peut et sera facilement augmentée par les exploitants de la plateforme.

L'alinéa 2 doit donc être supprimé :

> ~~[2] Elles peuvent diviser les documents dépassant 64 mégaoctets en plusieurs documents de 64 mégaoctets au plus et soumettre ceux-ci à un contrôle antivirus.~~

Ad alinéa 4

Une déclaration claire, lorsque le dépistage des virus n'a été effectué que de manière limitée, est absolument nécessaire.

La manière dont les résultats du dépistage des virus sont communiqués aux utilisateurs n'est en l'état pas claire. Cette communication doit être simple sur le plan technique et facile à comprendre sur le fond.

L'alinéa 4 devrait donc être libellé comme suit :

> [4] Les documents qui n'ont pas été soumis à un contrôle antivirus ~~au sens de l'al. 2 ou~~ ou qui ont été soumis à un contrôle antivirus limité doivent être identifiés en tant que tels.

Ad alinéa 5

Lorsque la plateforme informe l'expéditeur qu'un document n'a pas pu être transmis, le motif de la non-transmission devrait être précisé (voir ci-dessus les commentaires à l'art. 5 al. 2 let. d ch. 2).

Ad article 15 **Calcul de l'émolument**

Remarque générale sur le calcul des émoluments

Le calcul des émoluments se fonde sur les articles 6 et 32 de la LPCJ. Les coûts de la plateforme sont répartis entre les cantons utilisateurs. Pour les membres de la corporation, la part des émoluments est calculée sur la base de la population résidante permanente. Avec les non-membres, la corporation conclut une convention conformément à l'article 6 de la LPCJ. L'indemnisation

convenue doit couvrir l'ensemble des frais (y compris les frais d'investissement, FF 2023 679, p. 22) occasionnés par les non-membres. Les coûts pour les non-membres seront donc généralement plus élevés que ceux des membres.

Ad alinéa premier

Il y a lieu d'harmoniser les versions allemande et française de cette disposition, dont la cohérence terminologique doit en outre être garantie. Pour plus de clarté, il est proposé de scinder l'alinéa 1 en deux alinéas, le texte proposé étant le suivant :

> *[1] Le montant total de l'émolument annuel dû ~~pour l'utilisation de la plateforme centralisée couvre les frais d'exploitation et de développement de la plateforme~~ par les membres de la corporation de droit public doit couvrir les frais d'exploitation et de développement ~~de~~ de la plateforme centralisée ~~et~~ et permet la constitution d'une réserve correspondant à 10 % des frais d'exploitation annuels pour assurer la liquidité de la corporation de droit public. ~~Les recettes versées par les cantons qui ne sont pas membres de la corporation pour les prestations auxquelles ils recourent sont déduites du calcul du montant total de l'émolument~~.*
> *[2] Les contributions versées par les cantons qui ne sont pas membres de la corporation de droit public sont déduites du montant total de l'émolument.*

Ad alinéa 3 (alinéa 2 du projet)

L'alinéa 2 du projet devient l'alinéa 3. Il est en outre proposé de le modifier comme suit :

> *[3] Le DFJP fixe le montant ~~annuel~~ total de l'émolument annuel à l'avance, tous les trois ans, ~~en se fondant~~ sur la base de la planification financière de la corporation de droit public.*

Ad alinéa 4 (alinéa 3 du projet)

L'alinéa 3 du projet devient l'alinéa 4. Il est en outre proposé de le modifier comme suit :

> *[34] Le DFJP peut adapter l'émolument pendant la période visée à l'al. ~~2~~ 3 s'il constate que les contributions encaissées par la corporation au sens des al. 1 et 2 ~~il~~ ne couvrent pas les frais d'exploitation et de développement de la plateforme ou que la réserve dépasse la limite fixée à l'al. 1.*

Ad article 16 Répartition de l'émolument

Selon l'état actuel de la planification, l'administration fédérale utilise la plateforme pour les procédures pénales administratives de la Confédération. La part fédérale de 10% est donc jugée appropriée. Une fois l'obligation pleinement mise en œuvre, il conviendra d'examiner si l'utilisation effective correspond au modèle d'émolument proposé ou s'il y a lieu d'adapter la répartition des émoluments, notamment au regard du nombre de transmissions relevant du droit pénal administratif. Une révision du mode de calcul de l'émolument est d'ailleurs prévue à l'article 21. La répartition de l'émolument devrait également faire l'objet d'un examen.

Le canton de Genève est favorable à la répartition en fonction de la population résidente permanente prévue à l'alinéa 2. Toutefois, il souligne que seules les données statistiques disponibles au moment du calcul peuvent servir de base. Sur la base de ces données contraignantes, le DFJP fixera le montant annuel des émoluments. Il tiendra compte à cet égard des seuils définis à l'article 15, alinéa 4, ainsi que de l'adhésion éventuelle d'un non-membre à la corporation justitia.swiss après sa création (cf. art. 19 de la convention justitia.swiss ainsi que le rapport explicatif relatif à la convention justitia.swiss, p. 17).

La formulation suivante est proposée :

[1] Le montant total de l'émolument est réparti comme suit entre la Confédération et les cantons membres de la corporation de droit public :
a. administration fédérale et Ministère public de la Confédération (MPC) : 5 % ;
b. tribunaux de la Confédération : 5 % ;
c. cantons : 90 %.
[2] La part des cantons est répartie entre les cantons qui sont membres de la corporation de droit public proportionnellement à leur population résidente permanente au ~~moment de la fixation de l'émolument~~ 1er janvier de l'avant-dernière année pour laquelle l'émolument est dû; est déterminant le nombre d'habitants selon la loi fédérale du 9 octobre 1992 sur la statistique fédérale, la loi du 22 juin 2007 sur le recensement et les ordonnances qui s'y rapportent.
[3] Le DFJP fixe chaque année la répartition de la taxe entre les cantons.

Ad article 19 **Échéance**

L'ordonnance laisse ouvertes les autres modalités d'exécution. On peut supposer que les règles du code des obligations s'appliquent par analogie.

Il est donc proposé d'adopter le libellé suivant pour cette disposition :

[1] L'émolument annuel ~~facturé aux~~ des membres de la corporation de droit public doit être versé à l'avance et est dû le 1er janvier.
[2] L'émolument ~~pour la première année d'exploitation de la corporation de droit public est dû le jour de l'entrée en vigueur~~ pour l'utilisation de la plateforme centrale est dû pour la première fois à la date d'entrée en vigueur de la présente ordonnance.
[3] Les dispositions du Code des obligations relatives à la demeure du débiteur s'appliquent par analogie.

Ad article 22 **Numérisation de documents physiques**

Cette disposition concerne toutes les autorités qui mènent des procédures dont le droit procédural est soumis à la LPCJ (art. 2 LPCJ). Pour les cantons, ce sont le code de procédure civile, la loi sur l'aide aux victimes et le code de procédure pénale qui priment.

L'alinéa 3 prévoit la reconnaissance de texte. Celle-ci semble judicieuse dans de nombreux cas et facilite le traitement des documents. Pour les textes en langue étrangère, le résultat de la reconnaissance de texte peut toutefois s'avérer insatisfaisant ou erroné selon l'état actuel de la technique. Les spécifications techniques de la numérisation devraient figurer dans une ordonnance départementale, étant précisé que la seule mention d'une résolution minimale ne semble pas suffisante pour garantir la qualité de la reconnaissance de texte.

Ad article 22a (nouveau) **Renvoi de documents physiques (nouveau)**

Problématique

Le chiffre 2.6 du rapport explicatif relatif à l'ouverture de la procédure de consultation (p. 7) indique qu'il a été renoncé à intégrer dans l'ordonnance une disposition relative à l'interprétation restrictive de l'article 30 LPCJ car il n'y aurait plus de marge de manœuvre légale à cet effet. Cette constatation

se réfère à l'interprétation de la notion de « documents » figurant à l'article 30, qui n'est distinguée dans la loi ni par domaine juridique ni par contenu des documents.

Une approche différenciée est toutefois nécessaire, selon l'avis défendu ici, afin de ne pas créer, avec une ordonnance lacunaire relative à la LPCJ, des problèmes qui n'existent pas dans le monde analogique. Cela signifie également que, selon l'avis défendu ici, les lois de procédure applicables laissent sans nul doute une marge d'interprétation téléologique des dispositions de la LPCJ.

En particulier dans la procédure pénale, les documents déposés physiquement ne sont renvoyés à leur expéditeur que dans des cas exceptionnels. Les services de police et les ministères publics continueront de recevoir chaque année, même après l'entrée en vigueur des modifications des lois de procédure applicables, des milliers de plaintes et autres documents similaires sous format papier, car ces requêtes émanent généralement de particuliers qui ne souhaitent pas s'inscrire au préalable sur la plateforme « justitia.swiss ». Cette quantité considérable de documents est rédigée spécialement à l'intention des autorités pénales et souvent complétée par des photocopies de documents pertinents sur le plan juridique. Dans les deux cas, la source ou l'original reste chez l'expéditeur.

Si la LPCJ n'est pas interprétée de manière restrictive, ce qui, selon les explications relatives à l'avant-projet actuel, ne devrait pas être le cas, la LPCJ instaurera de nouvelles obligations de renvoi, qui n'existent pas dans le monde analogique. Cela ne peut pas avoir été la volonté du législateur.

Le renvoi de documents n'a aucune utilité si la finalité d'un document se limite à la transmission du message qu'il contient. Les expéditeurs de ces messages disposent déjà de copies de leurs demandes ou des originaux dont ils ont fait des photocopies. Les exemplaires renvoyés seront donc jetés dès qu'ils seront revenus chez leurs expéditeurs d'origine.

Même dans le cas, plutôt rare, où des divergences surgiraient a posteriori quant à savoir si les copies numérisées figurant dans les dossiers administratifs correspondent aux documents déposés, les documents renvoyés ne pourraient pas servir de preuve, car il serait impossible de déterminer si ce sont bien ces documents qui ont été déposés auprès de l'autorité.

La distinction entre les simples communications et les documents qui, outre le contenu de la communication, comportent un contenu supplémentaire, est déjà prévue dans la LPCJ.

L'article 30, alinéa 2, LPCJ prévoit que les documents peuvent être conservés par les autorités s'ils sont encore nécessaires dans le cadre de la procédure. Il ressort du message y relatif du 15 février 2023 (FF 2023 679ss) que les documents ayant valeur de titre ne doivent pas être renvoyés immédiatement (commentaires relatifs à l'art. 30 P-LPCJ, p. 35). Cela signifie également que l'obligation de renvoyer les actes officiels, dont la restitution présente un intérêt pour les expéditeurs, n'est pas remise en cause en l'espèce.

En revanche, il n'est pas nécessaire de préciser davantage que l'interprétation de la LPCJ au sens d'un nouvel échange postal sous forme papier entraînerait une charge supplémentaire considérable en termes de frais de port et de travail. Une interprétation de la loi qui conduit en fin de compte à ce que des milliers de liasses de vieux papiers doivent être affranchies ne peut être justifiée par l'intention du législateur.

Solution proposée

Pour les raisons susmentionnées, il est proposé en l'espèce d'insérer un nouvel article 22a. La formulation choisie précise que les documents conservés conformément à l'article 30, alinéa 2, LPCJ ne sont pas exemptés de l'obligation de renvoi. Si, en revanche, l'un des critères mentionnés ci-après s'applique, il est certain que l'expéditeur ne tire aucune valeur ajoutée d'un renvoi, raison pour laquelle il est nécessaire, en se référant à l'objectif normatif du législateur, d'inscrire dans

l'ordonnance une interprétation restrictive de la notion de document conformément à l'article 30 LPCJ. Si l'expéditeur a un intérêt à ce que le document lui soit renvoyé, il peut en faire la demande au préalable.

Article 22a Renvoi des documents physiques

Sauf demande préalable en ce sens de la part de l'expéditeur ou de l'expéditrice, les pièces du dossier sont exemptées de l'obligation de renvoi des documents remis physiquement, prévue à l'article 30, alinéa 1, LPCJ, s'ils ne relèvent pas de l'article 30, alinéa 2, LPCJ et s'ils ne doivent pas être signés à la main conformément au droit procédural applicable ou s'ils ont la même valeur probante sous forme numérisée, à savoir les impressions de documents créés électroniquement ou les photocopies.

Ad article 22b (nouveau) **Notification de copies papier de documents originaux générés par voie électronique (nouveau)**

Problématique

Le chiffre 2.6 du rapport explicatif relatif à l'ouverture de la procédure de consultation (p. 7) précise que l'idée de garantir la notification des décisions finales signées électroniquement par l'envoi de copies papier a été écartée, car les dispositions légales applicables ne le permettaient pas. Concrètement, il s'agit du fait que l'article 353, alinéa 1, lettre k, nCPP prescrit, pour l'ordonnance pénale du ministère public : *« L'ordonnance pénale contient les informations suivantes : (...) la signature de la personne qui a établi l'ordonnance, si elle est notifiée sur papier. »* L'article 238, lettre h, nCPC contient une disposition similaire pour les décisions des tribunaux civils.

L'article 22 concrétise l'article 29 LPCJ (numérisation des documents physiques) et donc le passage du support papier au dossier électronique. Le processus inverse n'est toutefois pas décrit dans la LCPJ, bien qu'il s'agisse en pratique d'une exigence très importante, car selon le concept de base de la LPCJ, la création électronique de dossiers doit être la norme.

Toutefois, lorsque des particuliers ne souhaitent pas s'inscrire sur une plateforme de transmission électronique, ils conserveront à l'avenir le droit de se voir remettre un exemplaire papier des communications et des décisions. En particulier, les autorités pénales chargées des contraventions et les ministères publics rendent chaque année des dizaines de milliers de décisions définitives. Si ces procédures sont exclues de la gestion électronique des dossiers parce que, selon l'interprétation (désormais abandonnée) des dispositions procédurales applicables de l'ordonnance, il faudrait tout de même les traiter sur papier, il ne resterait alors qu'un volume compris entre 10 et 20 % des dossiers qui pourront être gérés par voie électronique. C'est notamment dans le domaine des affaires de masse que le potentiel de rationalisation de la digitalisation s'évapore.

Certes, la LPCJ repose sur le principe réglementaire selon lequel les particuliers ne doivent pas être contraints de communiquer par voie électronique avec les autorités, et il ne s'agit donc pas ici de remettre en cause ce principe. En revanche, il ne peut être juste d'interpréter l'exigence de signature de manière si restrictive qu'elle freine tout progrès, en contradiction avec la volonté du législateur.

Il ressort de l'article 22, alinéa 2, LPCJ qu'à l'avenir, un cachet électronique réglementé devra garantir qu'un document établi par voie électronique provient bien de l'autorité compétente, telle qu'elle ressort par exemple de l'en-tête ou d'un élément similaire. À propos de cet article, le message relatif à la LPCJ précise : « L'exigence de signature constitue souvent un obstacle à la numérisation. Au lieu de la signature, la loi prévoit l'authentification à l'aide d'un moyen d'identification électronique reconnu ainsi que l'apposition d'un cachet électronique réglementé. » (Message relatif à la loi fédérale sur les plateformes de communication électronique dans le domaine judiciaire du 15 février 2023 ; FF 2023 679ss, remarques préliminaires concernant l'art. 22, p. 30). Il en résulte que le cachet électronique

réglementé remplace la signature manuscrite dans le cadre de la gestion électronique des dossiers. Il n'y a donc plus de place pour un recours à l'article 14 CO dans le champ d'application de la LPCJ. La LPCJ, en tant que loi plus récente et plus spécifique, remplace la signature manuscrite des membres des autorités par un cachet électronique réglementé (concernant le niveau de protection, cf. le message, *op. cit.*, ad art. 22 LPCJ).

Solution proposée

Il convient de donner raison au rapport explicatif accompagnant l'ouverture de la procédure de consultation sur ce point, dans la mesure où il ressort des lois de procédure applicables que, par exemple, les décisions définitives doivent porter la signature de la personne qui les a rendues lorsqu'elles sont envoyées en original sur papier. Selon l'avis défendu ici, cette formulation permet toutefois tout à fait une interprétation conforme à l'objectif manifeste et sans équivoque de la loi.

Aujourd'hui déjà, il est d'usage auprès des tribunaux civils et des autorités pénales de verser l'original des décisions définitives au dossier de l'autorité et de remettre aux parties une photocopie de l'original. Comme déjà mentionné plus haut concernant la disposition relative au renvoi des documents papier envoyés, c'est en renonçant à une interprétation restrictive qu'une nouvelle obligation est créée dans le monde analogique. Si l'on suit le rapport explicatif, il y aurait soudainement une obligation d'envoyer des originaux papier. Cela multiplierait de manière exponentielle l'envoi d'originaux papier dans le monde numérique.

Cela ne peut avoir été l'intention du législateur.

En conséquence, il convient de préciser dans l'ordonnance que la notification des documents nécessitant une signature à des personnes qui ne sont pas enregistrées sur la plateforme peut bien sûr continuer à se faire, à l'avenir également, au moyen d'une copie papier de l'original (désormais établi par voie électronique), lequel reste dans le dossier numérique. Une copie papier de l'original électronique a exactement la même valeur informative qu'une décision portant une signature manuscrite. Si le destinataire a des doutes quant à l'authenticité de la décision, il peut à tout moment se faire envoyer l'original électronique ou se le faire présenter au siège de l'autorité, ce qui lui permet en outre de vérifier la date de création de l'original indiquée sur la copie papier.

La solution proposée présente l'avantage d'éviter qu'il n'y ait, dans une même procédure, deux originaux de la même décision coexistant parallèlement (par exemple lorsqu'une personne accusée est défendue et qu'un exemplaire muni d'un cachet électronique de la décision finale (sans aucune signature) pourrait lui être envoyé par l'intermédiaire de son représentant légal, alors que la partie civile n'est pas représentée par un avocat et qu'il faudrait lui envoyer une copie papier qui, à son tour, devrait porter une signature manuscrite). En outre, cela créerait une situation juridique identique à celle de la juridiction fédérale. La LPCJ n'exige justement pas que les jugements portent une signature lorsqu'ils sont envoyés sur papier.

Pour les raisons exposées au point 3.1, il est donc proposé d'insérer un nouvel article 22b:

> ***Article 22b*** *Notification de copies papier de documents créés par voie électronique*
>
> *Les autorités qui gèrent leurs dossiers par voie électronique apposent un cachet électronique réglementé sur les documents pour lesquels le droit procédural applicable prévoit, pour leur forme papier, la signature d'au moins un représentant de l'autorité, lorsqu'elles doivent envoyer ces documents. Dans la mesure où de tels documents doivent (également) être notifiés à des personnes avec lesquelles l'autorité ne communique pas par voie électronique, la transmission du document s'effectue au moyen d'une copie papier de l'original électronique. La notification de la copie papier fait courir le délai si les personnes destinataires sont informées sur la copie papier qu'elles peuvent*

obtenir gratuitement l'original électronique via une plateforme conformément à la LPCJ ou demander à l'autorité un double signé à la main.

Si l'on s'en tient à l'interprétation beaucoup trop restrictive de la LPCJ, telle qu'elle est esquissée dans les explications relatives au projet d'ordonnance, il faudrait au moins envisager l'utilisation d'une signature électronique qualifiée des membres de l'autorité (en plus du cachet de l'autorité) afin de satisfaire à la notion de « signature » utilisée dans les lois de procédure, bien que celle-ci, comme indiqué plus haut, ait été remplacée par le cachet de l'autorité dans le contexte de la gestion numérique des dossiers.

Modification du titre du chapitre 2

Au vu des propositions qui précèdent, le titre du chapitre 2 devrait être modifié comme suit :

Chapitre 2 Numérisation et renvoi de documents physiques, envoi papier de documents créés par voie électronique

Ad articles 23 et 24

Problématique

Les autorités judiciaires ont sollicité et obtenu, pendant les travaux parlementaires portant sur la LPCJ, que certaines communications entre autorités, sur un plan intracantonal (procédure civile) ou même intercantonal (procédure pénale), puissent intervenir sous forme électronique sans recourir à une plateforme au sens de la LPCJ. La manière dont le projet d'ordonnance concrétise cette alternative autorisée est incompréhensible. Le champ d'application respectif des articles 23 et 24 du projet n'est pas défini. Les exigences posées à l'article 23 réduisent à néant l'intérêt de toute communication électronique alternative et imposent aux autorités judiciaires des conditions et modalités aussi restrictives que la plateforme, alors même que cette voie différente devrait permettre des échanges facilités entre autorités, sans impact procédural pour les parties. La formulation proposée paraît reposer sur une méconnaissance du terrain et des processus judiciaires. Son maintien aboutirait nécessairement à des problématiques pratiques difficilement surmontables et à des contentieux supplémentaires.

Le canton de Genève invite l'office fédéral de la justice à reprendre langue avec le projet Justitia 4.0 et son groupe d'experts, de manière à clarifier les besoins et les cas métier envisagés par les autorités judiciaires lorsqu'elles ont sollicité des commissions parlementaires une voie alternative à l'usage d'une plateforme pour certaines communications entre autorités. Il y aura dans tous les cas lieu de tenir compte des remarques qui suivent.

Ad article 23 Exigences

Cette disposition concrétise l'article 128b, alinéa 2, du Code de procédure civile (CPC), l'article 103b, alinéa 2, du Code de procédure pénale (CPP) et l'article 8c, alinéa 2, de la loi sur l'aide aux victimes du 23 mars 2007 (LAVI).

Cette disposition devrait viser la communication entre les autorités pénales au sein de la chaîne de procédure pénale, dans le cadre de laquelle les dossiers doivent par exemple être transmis à l'instance supérieure en cas de recours, lorsque d'autres autorités sont chargées de certains actes de procédure (ex. mandat d'acte d'enquête du ministère public à la police ou lors de la transmission des rapports de police au ministère public).

Un deuxième champ d'application est la chaîne civile, par exemple lorsqu'un tribunal civil ordonne à l'office des poursuites, à l'office des faillites ou à l'office du registre du commerce d'accomplir un acte

déterminé ou lorsque le tribunal de première instance transmet ses dossiers à l'instance cantonale supérieure en raison d'un recours.

La transmission physique des dossiers entre les autorités pénales s'effectue actuellement par la Poste, par courrier interne ou par porteur. Le mandat d'acte d'enquête confié à la police pour une mesure d'instruction est généralement formulé par écrit mais l'heure exacte de son expédition et de sa réception n'a pas d'importance. De la même manière, la police transmet au ministère public ses rapports sans enregistrement de l'heure et sans délivrance de quittance. Ces communications internes n'ont pas d'impact procédural et ne modifient pas les droits et obligations des parties. Les exigences posées par le projet ne se justifient aucunement.

Les dispositions d'exécution proposées s'inspirent fortement de la solution technique de la plateforme. Pour la transmission électronique au sein du canton (CPC) ou entre autorités pénales (CPP), il faut toutefois appliquer d'autres exigences que pour la communication via la plateforme. La transmission électronique au sein d'un canton pourra par exemple s'effectuer à l'avenir par la modification des droits d'accès à la base de données cantonale commune. Pour cela, aucune quittance n'est nécessaire. L'enregistrement dans les logfiles du système informatique cantonal suffit. Du point de vue de la protection des données et de la sécurité informatique, la modification des droits d'accès est clairement préférable à l'envoi répété de documents via une plateforme externe.

L'article 23 doit en outre être complété de manière à autoriser la transmission électronique de documents par la modification des droits d'accès à une base de données commune. La traçabilité des moments de la transmission ou des moments de la modification des droits d'accès doit être garantie. Les exigences du CPC et du CPP ne vont pas jusqu'à rendre nécessaire, dans le cadre du passage au numérique, un horodatage synchronisé comme celui prévu à la lettre b. Il convient donc de renoncer à ce critère.

Ad article 24 Transmission par voie électronique entre les autorités

Comme indiqué, le champ d'application de cette disposition n'est pas défini et son articulation avec l'article 23 est obscure.

L'intitulé est trop général et donc trompeur. Il s'agit toujours de communications émanant des autorités pénales ou destinées à celles-ci, ou des tribunaux civils ou à destination de ceux-ci, dans le cadre de procédures relevant du CPP ou du CPC. Parallèlement, il semble nécessaire de définir la notion des autres autorités, c'est-à-dire celles qui sont soumises à l'obligation de communiquer par voie électronique avec les autorités pénales (cf. supra ad article 6).

Ad article 28 Entrée en vigueur

Le financement du projet Justitia 4.0, qui met en place la plateforme centrale pour le compte des cantons, de la Confédération et des autorités judiciaires, est assuré jusqu'à fin 2027. Le financement de la plateforme sera donc assuré par des émoluments à partir de début 2028. L'ordonnance devrait donc entrer en vigueur en même temps que l'entrée en vigueur finale de la loi afin de permettre la planification financière des cantons à partir de 2028.

III. Fin d'accréditation des autres moyens de communication électronique dans le cadre de procédures civiles et pénales

Le canton de Genève insiste pour que la plateforme justitia.swiss soit le moyen de communication exclusif dans les procédures civiles et pénales et qu'aucune phase transitoire ne soit prévue permettant d'opter pour les moyens actuels (PrivaSphère et IncaMail).