



Explication des dispositions

Art. 1 Objet de champ d'application

Le 1^{er} alinéa circonscrit le champ d'application de l'ordonnance. Celle-ci ne vaut que pour la communication électronique dans le cadre d'une procédure administrative fédérale. Elle ne s'applique donc pas aux procédures qui ne sont pas régies par la loi sur la procédure administrative fédérale (PA, RS 172.021), qu'il s'agisse de procédures pénales ou de procédures administratives auxquelles la PA ne s'applique pas (cf. art. 3 PA) à l'instar de la procédure de dédouanement. En matière d'assurances sociales, l'applicabilité de l'ordonnance dépendra de la mise en œuvre de l'art. 55, al. 1^{bis}, LPGA (RS 830.1).

L'ordonnance ne vaut par ailleurs que pour les communications entre une partie à la procédure et l'autorité administrative fédérale compétente (al. 1). Elle ne concerne pas les communications entre autorités fédérales ou les communications avec des autorités cantonales, même si ces communications se déroulent dans le cadre d'une procédure administrative. La demande d'avis à une autre autorité fédérale et la communication de cet avis ne sont pas régies par la présente ordonnance. Demeure réservée l'hypothèse où une autorité aurait le statut de partie à la procédure, par exemple parce qu'elle aurait la qualité pour recourir contre la décision rendue à l'issue de la procédure (art. 6 PA).

L'ordonnance s'applique aux communications écrites relatives à des actes de procédure. Elle concerne la communication de tout document comprenant du texte ou des images qui doit être porté au dossier parce qu'il peut être déterminant pour le déroulement ou l'issue de la procédure (par ex. document transmis aux fins de preuve, expertise) ou constitue une étape formelle de la procédure (par ex. demande ouvrant la procédure, décision finale de l'autorité). L'ordonnance ne s'applique pas aux communications écrites qui sont faites en dehors d'une procédure (par ex. une simple demande d'information) ni aux communications relatives à des prestations offertes sans décision. Elle ne concerne pas non plus la communication orale par voie électronique (voice over IP).

Art. 2 Plateformes reconnues de messagerie sécurisée

La méthode de base de communication électronique qui est prévue par l'ordonnance est, en particulier pour la notification des décisions, l'envoi par une plateforme de messagerie sécurisée. Une telle plateforme comporte de nombreux avantages par rapport au courrier électronique (courriel) ordinaire. Elle permet en effet de garantir l'identification de l'expéditeur et du destinataire, d'assurer la confidentialité et l'intégrité des communications ainsi que de donner force probatoire tant à l'envoi qu'à la réception du message.

Vu les frais considérables qu'entraîneraient le développement et la gestion d'une plateforme de messagerie sécurisée par l'administration fédérale, il est prévu d'utiliser les services de plateformes commerciales, à l'instar de ce que fait le Tribunal fédéral

en recourant à la plateforme Incamail commercialisée par la Poste. Il n'est pas opportun de prévoir l'usage de la seule plateforme Incamail, car d'autres fournisseurs de messagerie sécurisée peuvent développer des plateformes qui sont plus performantes ou mieux adaptées à des besoins spécifiques d'autorités fédérales. Il faut néanmoins canaliser le choix de la plateforme en prévoyant une procédure de reconnaissance. Cette procédure permet d'une part de garantir la qualité des plateformes et ainsi d'éviter que chaque autorité doive contrôler si la plateforme qui lui est proposée permet l'identification des participants, la confidentialité des communications et leur non répudiabilité (al. 2, let. a et b) et assure le respect des exigences de la PA (al. 2, let. c). La procédure de reconnaissance permet aussi d'imposer l'interopérabilité de toutes les plateformes utilisées par les autorités fédérales, de sorte que les personnes privées pourront, en s'inscrivant auprès d'une plateforme reconnue, communiquer avec les autorités fédérales même si celles-ci utilisent d'autres plateformes. En pratique, cette interopérabilité est assurée par la compatibilité des protocoles de communication utilisés par les plateformes reconnues (al. 1, let. e) et par un routage des communications d'une plateforme à l'autre en fonction de l'expéditeur et du destinataire (al. 1, let. d). Le protocole « OSCI-Transport » a été développé par la OSCI-Leitstelle sur mandat des collectivités publiques allemandes pour assurer une communication sûre aux administrations publiques (cf. www1.osci.de). Les plateformes de messagerie sécurisée qui souhaitent être reconnues doivent remplir les exigences de la technique du standard OSCI, donc être conformes au dernier développement de ce protocole. Le protocole OSCI permet de gérer de manière automatisée la communication entre les particuliers et les autorités et de garantir l'enregistrement des moments déterminants de la communication. Le choix du protocole OSCI permet aussi de garantir une harmonisation de l'interface pour les utilisateurs. L'ordonnance n'exclut toutefois pas qu'une plateforme puisse reposer sur un autre protocole de communication pour autant que celui-ci est compatible avec le protocole OSCI.

Dans la mesure où le département fédéral des finances a déjà des compétences transversales en matière d'informatique, l'al. 2 lui attribue la tâche de statuer sur les demandes de reconnaissance des plateformes de messagerie sécurisée. Actuellement seuls deux fournisseurs (Incamail de la Poste et PrivaSphere SA) semblent entrer en ligne de compte.

La gestion du routage entre les plateformes reconnues devrait être assumée par l'une des plateformes reconnues. C'est pourquoi l'al. 5 permet au DFF de conclure un contrat avec l'une des plateformes reconnues pour la prise en charge de cette tâche.

Chapitre 2 Communication d'écrits à une autorité

Art. 3 Admissibilité

Cette disposition limite le cercle des autorités auxquelles les parties peuvent valablement communiquer des données par voie électronique, conformément à la disposition finale de la modification du 17 juin 2005 de la loi sur la procédure administrative. L'ordonnance ne mentionne pas elle-même les autorités avec lesquelles la communication électronique est possible, mais elle renvoie à un répertoire accessible via internet dans lequel ces autorités sont inscrites. Cette solution permet d'éviter de devoir modifier l'ordonnance et donc de passer devant le Conseil fédéral pour chaque autorité qui souhaite permettre la communication électronique. Il est ainsi possible d'étendre progressivement le cercle des autorités accessibles par voie électronique.

Afin de répondre au souhait d'autorités administratives fédérales, la possibilité est donnée de limiter l'admission de la communication à certaines procédures administratives.

Art. 4 Répertoire

Afin d'informer les particuliers sur les autorités administratives fédérales avec lesquelles la communication électronique est possible, il est prévu que soit publié un répertoire online des autorités admettant la communication électronique. Logiquement, ce répertoire devrait être intégré dans le portail www.admin.ch qui est géré par la Chancellerie fédérale. Le répertoire permet l'inscription pour chaque autorité de diverses informations et adresses nécessaires pour la communication électronique (al. 2).

L'ordonnance laisse les autorités libres de choisir les canaux de communication qu'elles veulent autoriser. L'al. 2, let c, énonce à titre exemplatif trois canaux : plateforme de messagerie sécurisée, site de saisie en ligne et courrier électronique ordinaire. Le choix d'un canal peut valoir de manière générale pour toutes les procédures devant une autorité ; il peut aussi être différent suivant la procédure en cause, voire même pour des phases de procédure. Cette solution permet de tenir aisément compte de l'évolution technologique sans devoir modifier à chaque fois l'ordonnance.

Art. 5 Format

L'ordonnance n'impose pas un format uniforme. Les situations sont en effet trop différentes selon le canal de communication utilisé. Les besoins ne sont pas les mêmes entre un site de saisie en ligne et un écrit transmis par messagerie sécurisée. Ils ne sont pas non plus les mêmes lorsque le document à envoyer contient du texte ou uniquement une image. Les autorités pourront ainsi publier dans le répertoire pour chaque canal de communication les formats autorisés (cf. art. 4, al. 2, let. e) que les particuliers devront utiliser (al. 1). En principe, il devrait s'agir du format PDF (Portable Document Format). Il s'agit d'un format de fichier informatique qui est ouvert et dont les spécifications sont publiques et utilisables librement et gratuitement (y compris pour la création de documents PDF par l'usage d'un des nombreux logiciels gratuits à cet effet). Il peut être utilisé sur la plupart des systèmes informatiques. Il permet la création de fichiers fidèles aux documents originaux et préserve les informations du fichier source— texte, dessins, images — quelle que soit l'application utilisée pour créer celui-ci. L'origine du document PDF peut aussi bien être un document électronique (par ex. un document Word) qu'un document papier qui a été scanné. En vertu de l'art. 52 PCF (RS 273 tel que modifié par la loi sur le Tribunal fédéral) en relation avec l'art. 19 PA, les parties à une procédure administrative sont en effet en droit d'envoyer aussi une copie électronique d'un document papier.

Les autorités devront veiller lors du choix du format à permettre l'archivage des documents qui leur sont envoyés. Il faut relever que le format PDF ne garantit pas en lui-même l'archivage à long terme. Une variante du PDF (le PDF/A) a été développée à cette fin. Lorsque les outils de création de cette variante se seront suffisamment généralisés pour que l'on puisse exiger des particuliers qu'ils remettent leurs écrits et annexes dans ce format spécifique, les autorités devraient lui donner la préférence.

Un des avantages de la communication électronique est de faciliter le traitement subséquent des actes de procédure par l'autorité. Cet avantage est encore plus net en cas d'usage d'un formulaire structuré, car la reprise des données peut être automatisée. L'al. 1 permet à l'autorité de mettre à disposition sur son site internet un formulaire électronique (tel qu'un formulaire XML). Dans un tel cas, toutefois, l'autorité devrait aussi mettre à disposition un programme gratuit qui permet de consulter le formulaire, de le remplir et de produire le document à transférer à l'autorité.

Lorsqu'un document envoyé contient un virus ou un autre programme nuisible, le contenu du message est usuellement intercepté par la protection mise en place par l'autorité et ne pourra pas être lu. De même, lorsque les documents contiennent des représentations visuelles (images ou graphiques) telles que des plans, il y a un risque que la lisibilité du document ne soit réduite pour des motifs de facilitation de la communication par voie électronique ; le poids informatique de tels documents est souvent considérable, de sorte que les versions envoyées électroniquement via internet sont usuellement réduites considérablement, ce qui exclut l'impression à la taille originale et rend difficile la consultation sur écran de ces pièces. L'al. 2 permet à l'autorité d'exiger la réexpédition des documents sous un format qu'elle spécifie au cas par cas (par exemple un document TIFF avec une résolution minimale spécifique) ou de renvoyer les documents concernés par la poste après impression. Il en va de même si les documents ne sont pas dans le format requis par l'autorité. Il faut relever que l'autorité peut en outre, en vertu de l'art. 52 PCF en relation avec l'art. 19 PA, exiger la production du document papier original si la partie a envoyé une copie électronique de ce document.

A des fins de protection des données, l'al. 3 oblige les autorités à veiller au chiffrement des données lors de l'ouverture de canaux de communication aux particuliers. Ce chiffrement garantit qu'aucun tiers non autorisé ne puisse prendre connaissance de données personnelles contenues dans un écrit adressé à une autorité. Lors de la mise en place d'un site de saisie en ligne, le chiffrement sera assuré par exemple par un canal SSL entre le serveur de l'autorité et le butineur (browser) de l'expéditeur. Lors de l'usage d'une messagerie sécurisée ou lors de l'envoi d'un simple courriel, l'expéditeur devra chiffrer les écrits avec une clé de chiffrement de l'autorité de sorte que seule celle-ci sera en mesure de les déchiffrer. La clé utilisée à cette fin ne doit pas être rattachée à une personne physique spécifique et peut donc reposer sur un certificat qui ne remplit pas les exigences de l'art. 7 de la loi sur la signature électronique. Le répertoire des autorités doit spécifier l'adresse où trouver le certificat contenant la clé de chiffrement (art. 4, al. 2, let. f). Le chiffrement n'est pas une condition de validité de la communication.

L'institut de la propriété intellectuelle bénéficie en vertu de diverses dispositions légales d'une délégation législative pour réglementer les détails techniques de la communication par voie électronique dans ses domaines de conséquences (cf. par ex. art. 40, al. 1, LPM, RS 232.11, et art. 7a OPM, RS 232.111). L'al. 4 tient compte de cette spécificité en réservant les prescriptions particulières de l'institut.

Art. 6 Signature

La loi sur la procédure administrative fédérale exige que le « document contenant les écrits » qui est communiqué par voie électronique par les particuliers aux autorités soit signé avec une « signature électronique reconnue » (art. 21a, al. 2, PA). Cette exigence s'applique aussi à des actes très formels tels que des mémoires de recours

pour lesquels la loi exige expressément la signature du recourant ou de son mandataire (art. 52 PA). Comme la signature électronique qualifiée est la seule qui est à proprement parler réglementée en droit fédéral par la loi du 19 décembre 2003 sur la signature électronique, il convient d'assimiler la signature électronique reconnue au sens de la loi sur la procédure administrative à une signature électronique basée sur un certificat qualifié émanant d'un fournisseur de services de certification reconnu au sens de la loi du 19 décembre 2003 sur la signature électronique (cf. aussi Message, FF 2001 4063).

L'art. 21a, al. 2, exige une signature électronique reconnue non seulement pour signer les écrits dont le droit fédéral requiert la signature, mais aussi pour certifier l'ensemble des écrits communiqués par voie électronique. Cette exigence de certification par la signature électronique n'a pas pour but de rehausser les conditions formelles de validité des écrits qui, s'ils étaient envoyés par voie postale, n'auraient pas besoin d'être signés. La certification par la signature électronique reconnue vise à utiliser deux des fonctions de cette signature : une signature électronique qualifiée permet en effet d'une part d'identifier l'expéditeur et d'autre part de garantir l'intégrité du document envoyé (cf. Message, FF 2001 p. 4202 s.). En 2007, il s'avère que ces deux fonctions peuvent aussi être assumées par d'autres moyens. Comme la signature électronique qualifiée n'est de loin pas aussi répandue que l'on avait escompté lors des travaux préparatoires de la loi, il faut, pour les écrits dont le droit fédéral ne requiert pas la signature, réinterpréter l'exigence de certification conformément au but de l'art. 21a, al. 2, PA : les modalités de la communication par voie électronique de tels écrits doivent permettre d'une part d'identifier l'expéditeur et d'autre part de garantir que le document reçu par l'autorité est resté inchangé entre l'expédition par la partie et sa réception par l'autorité. Peu importe en revanche la méthode utilisée pour assurer ces deux fonctions. Il peut s'agir d'une signature électronique qualifiée. L'autorité peut cependant utiliser d'autres moyens, tels que la sécurisation des communications dans le cadre d'un site de saisie en ligne. L'art. 6, al. 2, de l'ordonnance explicite dans ce sens la règle de l'art. 21a, al. 2, PA.

L'exigence d'une signature qualifiée dans les cas où la signature d'un document spécifique est requise pose en pratique certaines difficultés. L'obtention de certificats qualifiés par les particuliers est pour le moment plutôt difficile et coûteuse. De plus, les plateformes commerciales de messagerie sécurisée n'utilisent actuellement pas des certificats qualifiés pour valider les envois mais des certificats dits avancés qui permettent de créer des signatures avancées au sens de l'art. 2, let. b, de la loi sur la signature électronique. Afin de tenir compte de cette situation l'al. 3 assouplit l'exigence d'une signature qualifiée. Il donne à l'autorité la faculté de renoncer à exiger que soit corrigée l'absence de signature électronique reconnue. L'autorité pourra utiliser cette faculté lorsqu'il lui est possible par d'autres moyens d'identifier l'expéditeur avec certitude, en particulier lorsque l'expéditeur est enregistré auprès de la plateforme reconnue de messagerie sécurisée (cf. art. 2, let. a, de l'ordonnance). Demeure réservée la conséquence prévue par l'art. 52, al. 3, PA en cas d'absence de signature du recours, à savoir l'irrecevabilité du recours.

Art. 7 Certificat

La loi sur la signature électronique laisse les particuliers libres de renoncer à rendre public leur certificat sur l'annuaire du fournisseur de certification (art. 11, al. 2, SCSE). Dans un tel cas, l'autorité ne peut contrôler ni la titularité de la clé de signature utilisée ni la validité du certificat. Il faut donc que l'expéditeur joigne son certificat à l'expédition pour permettre ce contrôle. Demeure réservée l'hypothèse où

l'expédition passe par une plateforme de messagerie sécurisée qui stocke les certificats des personnes inscrites.

Chapitre 3 Notification de décisions

Art. 8 Principe

La loi sur la procédure administrative donne aux autorités la faculté de procéder à la notification par voie électronique de leurs décisions (art. 34, al. 1^{bis}, PA). Les autorités sont toutefois libres de renoncer à utiliser cette faculté, même si le destinataire de l'acte souhaite une notification par voie électronique.

L'art. 8 reprend l'exigence faite par l'art. 34, al. 1^{bis}, PA que le particulier ait accepté la notification par voie électronique. Il précise que cette acceptation doit être expresse : le fait que le particulier ait lui-même communiqué avec l'autorité par voie électronique ne suffit pas comme acceptation (implicite) de la notification par voie électronique (cf. Message, FF 2001 4068). La seule exigence de forme pour l'acceptation est qu'elle ait été faite par écrit et non pas par oral; vu les conséquences de la fiction légale de l'art. 20, al. 2^{bis}, PA, il appartient à l'autorité d'apporter la preuve de l'acceptation de la notification par voie électronique. La notion de communication par écrit n'équivaut pas à la forme écrite au sens de l'art. 13 CO : la signature de l'acceptation n'est pas exigée. L'acceptation en cochant une case à ce sujet dans un formulaire sur un site en ligne est suffisante. L'art. 8, al. 1, spécifie en outre que l'acceptation doit concerner la procédure en cause. Au regard de l'applicabilité de la fiction légale, il ne suffit pas d'une acceptation une fois pour toutes, indépendamment de l'autorité et de la procédure concernée. L'al. 2 de cette disposition permet cependant aux personnes qui sont régulièrement parties à une procédure administrative devant une même autorité ou qui représentent régulièrement des parties devant une même autorité d'accepter globalement que cette autorité leur notifie par voie électronique les décisions les concernant. La révocation de cette acceptation est possible en tout temps et prend effet dès qu'elle a été communiquée à l'autorité.

Art. 9 Modalités

L'al. 1 prévoit comme principe pour la notification par voie électronique l'usage d'une plateforme reconnue de messagerie sécurisée. Ce mode de communication garantit en effet l'enregistrement du moment où l'expédition entre dans la sphère de puissance du destinataire, de sorte que l'on peut apporter la preuve du départ du délai de recours. La deuxième phrase de l'al. 1 permet toutefois l'usage d'autres modes de notification pour tenir compte des besoins spécifiques des sites de saisie en ligne ainsi que de l'évolution des technologies. Il faut notamment que la communication soit chiffrée pour garantir la protection des données personnelles des parties et de tiers éventuels. Le chiffrement peut être fait par la clé publique de chiffrement du destinataire ou par un autre mode de chiffrement, tel qu'un canal sécurisé nécessitant un mot de passe. La principale hypothèse visée par la deuxième phrase de l'al. 1 est celle où l'édiction d'une décision demandée sur un site de saisie en ligne peut entièrement être automatisée de sorte que la décision peut immédiatement être prononcée sans intervention humaine à l'issue de la demande.

Le format imposé par l'al. 2 est le PDF/A tel que défini par le standard ISO 19005-1. Ce format a d'abord l'avantage de pouvoir, comme les autres formes de PDF, être lu par tout destinataire, quel que soit le système informatique qu'il utilise. Il assure en

outre la garantie de l'archivage à long terme de la décision envoyée, tant par l'autorité qui l'expédie que par ses destinataires.

L'al. 3 exige de l'autorité qu'elle signe la décision avec une signature électronique qualifiée. Les certificats qualifiés nécessaires pourront être obtenus auprès de l'OFIT qui escompte être reconnu conformément à la loi sur la signature électronique d'ici à juin 2007. Un assouplissement est cependant prévu pour les envois de masse : à l'instar de ce qui vaut pour la signature manuscrite, l'ordonnance permet dans ces cas de remplacer la signature électronique qualifiée par une signature électronique avancée qui peut être apposée de manière automatique. Même si l'objectif est d'utiliser uniquement des signatures électroniques qualifiées, la réalisation de cet objectif dans le contexte des procédures de masse soulève diverses questions d'ordre technique qui n'ont pas encore trouvé de réponses satisfaisantes. L'emploi de signatures électroniques avancées est dans ce contexte une solution provisoire dont l'opportunité devra être réévaluée durant les prochaines années.

Art. 10 Moment de la notification

Cette disposition clarifie dans le cas de la communication électronique le moment où la décision est réputée notifiée à son destinataire. Elle s'applique principalement dans l'hypothèse où la communication passe par une plateforme reconnue de messagerie sécurisée : la décision et ses annexes sont déposées par l'autorité dans une boîte postale électronique sur la plateforme reconnue à l'intention du destinataire ; si celui-ci se connecte avec cette boîte postale et retire la décision en l'important sur son ordinateur, la décision est considérée comme notifiée au moment du retrait. L'art. 10 s'applique aussi lorsque la décision est notifiée par un serveur de l'autorité sur lequel sont créées des boîtes postales électroniques auxquelles les destinataires des décisions peuvent se connecter en s'identifiant pour retirer la décision les concernant. Si la notification passe par un autre mode de communication (cf. art. 9, al. 1), il faudra appliquer l'art. 10 par analogie en fonction des modalités spécifiques de la communication.

Contrairement au règlement du Tribunal fédéral sur la communication électronique avec les parties et les autorités précédentes (art. 6, RS 173.110.29), l'ordonnance ne règle pas l'applicabilité de la fiction de notification de l'art. 20, al. 2^{bis}, PA en cas de notification par voie électronique. Il s'est en effet avéré impossible d'énoncer une règle uniforme. La situation est différente selon que le destinataire est enregistré sur la plateforme de messagerie sécurisée ou s'il ne l'est pas comme dans le cas d'Incmail public. Dans le premier cas, on peut estimer que la boîte postale électronique d'un client inscrit de la plateforme de messagerie s'apparente à la boîte postale physique du destinataire : le dépôt de la décision dans cette boîte postale électronique peut être considéré comme une première tentative infructueuse de distribution qui lance le délai de 7 jours prévu par l'art. 20, al. 2^{bis}, PA pour la fiction légale de réception. En revanche, lorsque le destinataire n'est pas un client enregistré de la plateforme de messagerie sécurisée, l'annonce faite à cette personne par un simple courriel qu'une décision a été déposée à son intention dans une boîte postale électronique créée spécifiquement pour cette communication ne peut pas équivaloir à un avis de réception déposé dans la boîte aux lettres physique, car il n'y a pas de preuve que le courriel a atteint cette personne jusqu'à ce que celle-ci se connecte à la boîte postale électronique pour retirer la décision. Il appartiendra donc à la pratique et à la jurisprudence d'évaluer l'applicabilité de la fiction légale de l'art. 20, al. 2^{bis}, PA lors d'une notification par voie électronique en fonction des modalités utilisées.

Art. 11 Disposition transitoire

Afin de garantir la possibilité de communiquer par voie électronique dès l'entrée en vigueur de l'ordonnance, il convient d'accorder une reconnaissance provisoire à la plateforme incamail de La Poste Suisse. Cette plateforme avait été élaborée initialement dans le cadre du projet govlink géré conjointement par le Tribunal fédéral, l'office fédéral de la justice et la Chancellerie fédérale. Elle a été reprise ensuite par la Poste. Elle est utilisée par le Tribunal fédéral comme canal unique de communication électronique avec les particuliers. Cela justifie l'octroi à cette plateforme d'un statut provisoire particulier. A la fin du délai transitoire, la plateforme Incamail devra être reconnue aux mêmes conditions que les autres plateformes pour pouvoir continuer à être utilisée dans les relations entre les autorités administratives fédérales et les particuliers.

Art. 12 Entrée en vigueur

L'entrée en vigueur est prévue pour le 1^{er} septembre 2007. L'ordonnance devra être revue au plus tard à l'échéance du délai prévu par la disposition transitoire de la révision du 25 juin 2005 de la loi sur la procédure administrative, donc au 31 décembre 2016. En effet, à ce moment, la communication électronique sera possible avec toutes les autorités administratives fédérales pour toutes les procédures administratives. Le concept sur lequel repose le chapitre 2 de l'ordonnance ne sera alors plus conforme à la loi et devra être adapté. Pour cette raison, il est prévu que l'ordonnance sera échue le 31 décembre 2016.