EMMA DELESTRADE,
avocate,
cabinet Seban avocats

DAVID CONERARDY,
avocat,
cabinet Seban avocats

Principe
Toute décision administrative doit être signée par son auteur afin de permettre son identification et d'assurer l'imputabilité juridique de l'acte.

Garanties
Dans ces conditions, le recours à la signature électronique n'est possible que si le procédé utilisé présente des garanties équivalentes à celles de la signature manuscrite.

Cadre de référence
Le référentiel général de sécurité constitue le cadre normatif national de référence pour la sécurisation des échanges électroniques au sein du secteur public.

Dématérialisation

La signature électronique des actes administratifs

La dématérialisation des procédures administratives s'est progressivement imposée comme un pilier de la modernisation de l'action publique. Au cœur de cette transformation, la signature électronique joue un rôle essentiel pour formaliser les décisions prises par les collectivités territoriales.

Destinée à garantir la sécurité et l'authenticité des actes, la signature électronique soulève toutefois des questions juridiques importantes concernant sa validité, la responsabilité du signataire ou encore les risques de contentieux en cas d'irrégularité.

Les collectivités territoriales sont donc amenées à concilier simplification administrative et respect d'un cadre normatif exigeant et complexe, notamment lorsque les élus cumulent plusieurs mandats.

PRINCIPE ET EXIGENCES APPLICABLES

Le principe est clair et constant : toute décision administrative doit être signée par son auteur pour permettre son identification et assurer l'imputabilité juridique de l'acte. L'article L.212-1 du code des relations entre le public et l'administration (CRPA) exige, à ce titre, que toute décision comporte la signature de son auteur, accompagnée, de manière lisible, de ses nom, prénom et qualité. La signature constitue donc une formalité substantielle conditionnant la régularité des actes administratifs.

Dans ces conditions, le recours à la signature électronique n'est possible que si le procédé utilisé présente des garanties équivalentes à celles de la signature manuscrite.

L'outil de certificat de signature électronique doit permettre, en particulier, d'identifier de manière certaine le signataire, d'établir un lien incontestable entre la signature et l'acte concerné, ou encore d'assurer l'intégrité du document après signature. Ces exigences résultent de l'article L.212 3 du CRPA et du Référentiel général de sécurité (RGS), qui fixent les normes juridiques et techniques applicables à la fiabilité des signatures électroniques.

Il n'existe donc aucune obligation pour les collectivités territoriales de recourir à la signature électronique. Il s'agit d'une simple faculté, dont la mise en œuvre est strictement encadrée et suppose le respect de standards techniques précis.

Le dispositif repose en particulier sur l'utilisation d'un certificat de signature électronique, élément central permettant d'identifier la personne physique signataire et de garantir la sécurité du procédé. La qualité du certificat conditionne directement la validité et la valeur probante de la signature électronique.

À NOTER

Le recours à la signature électronique n'est possible que si le procédé utilisé présente des garanties équivalentes à celles de la signature manuscrite.

RÉFÉRENTIEL GÉNÉRAL DE SÉCURITÉ

Le référentiel général de sécurité (RGS), créé par l'ordonnance n°2005 1516 du 8 décembre 2005, relative aux échanges électroniques entre les administrations, et complété par divers décrets d'application, constitue le cadre normatif national de référence pour la sécurisation des échanges électroniques au sein du secteur public.

Le RGS impose que tout procédé de signature électronique mis en œuvre par une administration garantisse l'identification fiable du signataire, l'existence d'un lien indissociable entre la signature et le document signé, ainsi que la détection de toute altération ultérieure du fichier.

Ce référentiel s'articule directement avec le règlement (UE) n°910/2014, dit règlement eIDAS, qui harmonise les niveaux de signature électronique au sein de l'Union européenne (simple, avancée, qualifiée) et organise leur reconnaissance mutuelle dans l'espace européen.

Ainsi, le RGS et le règlement eIDAS ne constituent pas des normes concurrentes, mais un ensemble cohérent et complémentaire : le RGS fixe les exigences techniques et opérationnelles applicables aux administrations françaises, tandis que le règlement eIDAS assure la reconnaissance uniforme des signatures qualifiées au niveau européen. L'élaboration et la mise à jour du RGS sont assurées par l'Agence

RÉFÉRENCES

- Règlement eIDAS, art. 26 à 29.
- Obtenir un certificat de signature électronique, Anssi.
- Guide de sélection du niveau des signatures et des cachets électroniques, Anssi.

nationale de la sécurité des systèmes d'information (Anssi).

Celle-ci joue également un rôle déterminant dans la mise en œuvre du règlement eIDAS: elle tient à jour la liste officielle des prestataires de services de confiance qualifiés, habilités à délivrer les certificats nécessaires à la création de signatures électroniques qualifiées. Cette liste, régulièrement actualisée, permet aux administrations d'identifier les prestataires dont les certificats répondent aux exigences les plus élevées du droit européen.

Le RGS prévoit trois niveaux de sécurité, permettant d'adapter le dispositif au degré de sensibilité des actes administratifs:
– RGS niveau 1 (élémentaire), adapté aux actes à faible risque, offrant une sécurité de base;
– RGS niveau 2 (standard), destiné aux actes présentant un risque moyen, avec une authentification renforcée;
– RGS niveau 3 (renforcé), requis pour les actes à forte valeur juridique ou à enjeux contentieux élevés, garantissant une identification certaine du signataire et une traçabilité complète.

Selon l'Anssi, les niveaux 2 et 3 du RGS se rapprochent du niveau de signature électronique qualifiée au sens du règlement eIDAS, tandis que le niveau 1 correspond davantage à une signature avancée.

L'absence de rattachement du procédé utilisé à un niveau du RGS permettant d'en démontrer la fiabilité fragilise la validité de l'acte administratif. Ainsi, une décision signée électroniquement, mais non conforme au RGS, expose son auteur à un risque d'irrégularité, notamment si la fiabilité du procédé ne peut être démontrée en cas de contestation.

Le Conseil d'État a d'ailleurs jugé qu'une candidature à un marché public dont la signature électronique n'offre pas de garanties techniques suffisantes quant à son authenticité doit être rejetée, faute de satisfaire aux exigences de validité de la signature.

SIGNATURE ÉLECTRONIQUE QUALIFIÉE

La signature électronique qualifiée constitue le niveau de garantie le plus élevé prévu par le droit européen. Elle repose sur un certificat qualifié délivré par un prestataire de services de confiance, lui-même qualifié au sens du règlement eIDAS, figurant sur la liste tenue par l'Anssi. Elle nécessite aussi l'utilisation d'un dispositif de création de signature qualifiée, assurant que les données de signature restent sous le contrôle exclusif de leur titulaire et ne peuvent être détournées ou altérées. Ce mécanisme permet en outre de détecter toute modification du document après signature, assurant une sécurité juridique maximale.

En droit français, lorsqu'un procédé respecte ces exigences européennes, il bénéficie d'une présomption légale de fiabilité. Celle-ci renforce la valeur probante de la signature et limite les contestations possibles, puisqu'il appartient alors à la partie qui en conteste la validité d'en démontrer l'irrégularité.

La cour administrative d'appel de Paris a rappelé la portée de cette présomption dans un litige relatif à un arrêté préfectoral refusant un titre de séjour. La requérante soutenait que la signature électronique apposée sur l'acte ne respectait pas les normes techniques du RGS. La cour a cependant jugé qu'un procédé qualifié, conforme à la réglementation applicable en la matière, devait être réputé fiable.

Après avoir constaté que la signature litigieuse avait été produite via un service qualifié figurant sur la liste publiée par l'Anssi, la cour d'appel a considéré que la charge de la preuve incombait à la requérante. Faute d'éléments de nature à renverser cette présomption, la décision administrative a été déclarée régulière.

Cette décision illustre non seulement la vigilance du juge administratif en ce qui concerne le respect des exigences techniques applicables aux signatures électroniques, mais également la force protectrice attachée à la signature qualifiée, qui contribue largement à sécuriser la valeur probante de l'ensemble des actes administratifs.

CARACTÈRE INDIVIDUEL DU CERTIFICAT QUALIFIÉ

L'Anssi rappelle que le certificat qualifié de signature électronique est strictement attaché à une personne physique, et non à une fonction, un service ou une collectivité. Il constitue un outil d'identification individuelle: c'est la personne qui signe, non l'institution.

Ce caractère personnel d'un tel certificat n'interdit cependant pas qu'un même titulaire utilise son certificat pour signer des actes pour le compte de plusieurs entités publiques, sous réserve du respect de deux conditions cumulatives:
- d'une part, que les règles d'usage fixées par le prestataire de services de confiance, ou à défaut, la politique interne de la collectivité, autorisent expressément un tel usage;
- d'autre part, que le signataire dispose effectivement, pour chacune des entités concernées, de la compétence, de l'habilitation ou de la délégation l'autorisant à engager juridiquement l'administration.

Il appartient donc aux collectivités territoriales de vérifier attentivement les conditions contractuelles liées au certificat et les règles qu'elles définissent elles-mêmes, afin de prévenir tout risque d'insécurité juridique lié à une utilisation inappropriée du même certificat pour plusieurs structures. Elles doivent également s'assurer que chaque acte signé électroniquement entre bien dans le périmètre des compétences du titulaire du certificat.

Ainsi, la combinaison du caractère personnel du certificat, du régime juridique protecteur attaché à la signature qualifiée et du contrôle du juge administratif constitue un ensemble cohérent visant à garantir la fiabilité et la sécurité des actes administratifs dématérialisés.●