RÉPUBLIQUE FRANÇAISE

Ministère de la culture et de la communication

Direction générale des patrimoines

Service interministériel des Archives de France

Note d'information DGP/SIAF/2011/018 du 18 octobre 2011

Parution de l'arrêté du 21 juin 2011 relatif à la signature numérique ou électronique en matière pénale

Le directeur, chargé des Archives de France

à

Mesdames et Messieurs les directeurs des services départementaux d'archives
sous couvert de Mesdames et Messieurs les préfets de région
et de Mesdames et Messieurs les préfets de département

Référence : arrêté du 21 juin 2011 relatif à la signature électronique ou numérique en matière pénale[1]

Par cette présente note d'information, je souhaite attirer votre attention sur la codification au sein du code de procédure pénale (partie « arrêtés », livre V bis) de l'arrêté du 21 juin 2011 relatif à la signature électronique ou numérique en matière pénale.

Ces dispositions précisent la portée de l'article 801-1 du Code de procédure pénale selon lequel : « *Tous les actes mentionnés au présent code, qu'il s'agisse d'actes d'enquête ou d'instruction ou de décisions juridictionnelles, peuvent être revêtus d'une signature numérique ou électronique, selon des modalités qui sont précisées par décret en Conseil d'État* », soit le décret n° 2010-671 en date du 18 juin 2010 (articles R. 249-9 à R. 249-12 du code de procédure pénale).

En effet ces dispositions accompagnent la dématérialisation d'actes relevant du domaine pénal (police, gendarmerie, justice) qui, dès lors qu'il seront revêtus d'une signature électronique, auront force probante. Il est remarquable qu'une des conditions découlant de cette dématérialisation soit **l'obligation d'archivage sécurisé, inscrite en tant que telle à l'article A53-6**.

Le dispositif s'articule ainsi autour de trois parties : une consacrée à la signature électronique (articles A. 53-2 à A. 53-4), une consacrée à la signature dite numérique (article A. 53-5) et une consacrée à l'archivage (article A. 53-6).

[1] http://www.legifrance.gouv.fr/affichTexte.do?idTexte=JORFTEXT000024248517&dateTexte=&categorieLien=id

1. La signature électronique

La signature électronique renvoie aux dispositifs du code civil (article 1316-4) selon lequel celle-ci n'est valablement apposée que par l'usage d'un procédé permettant l'identification du signataire, garantissant le lien de la signature avec l'acte auquel elle s'attache et assurant l'intégrité de cet acte. Cette signature doit ainsi être sécurisée au sens du 2 de l'article 1er du décret n° 2001-272 du 30 mars 2001 pris pour l'application de l'article 1316-4 du code civil relatif à la signature électronique, soit une signature électronique qui satisfait, en outre, aux exigences suivantes : être propre au signataire, être créée par des moyens que le signataire puisse garder sous son contrôle exclusif, garantir avec l'acte auquel elle s'attache un lien tel que toute modification ultérieure de l'acte soit détectable[2].

La signature électronique est apposée par les autorités chargées de l'action publique et de l'instruction.

Il est précisé que cette signature doit être conforme au référentiel général de sécurité qui fixe les règles auxquelles les systèmes d'information mis en place par les autorités administratives doivent se conformer pour assurer la sécurité des informations échangées, et notamment leur confidentialité et leur intégrité, ainsi que la disponibilité et l'intégrité de ces systèmes et l'identification de leurs utilisateurs. Ces règles sont définies selon des niveaux de sécurité prévus par le référentiel pour des fonctions de sécurité, telles que l'identification, la signature électronique, la confidentialité ou l'horodatage, qui permettent de répondre aux objectifs de sécurité mentionnés à l'alinéa précédent.

De même doivent être respectées les modalités du décret n° 2010-112 du 2 février 2010 pris pour application des articles 9, 10 et 12 de l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives, pour ce qui concerne l'homologation du système d'information qui met en œuvre la signature électronique ainsi que pour ce qui concerne la qualification des prestataires de services de certification qui délivrent des certificats électroniques ou encore la vérification des signatures elles-mêmes.

Les procédés de signature électronique doivent respecter les exigences du référentiel général de sécurité trois étoiles (***) pour les magistrats, agents du greffe et personnes habilitées pour les assister. En effet, une signature électronique sécurisée au sens de l'article premier du décret n°2001-272, établie avec un dispositif sécurisé de création de signature certifié conforme dans les conditions de l'article 3 de ce décret et mettant en œuvre des certificats de signature électronique conformes au niveau de sécurité (***) est *de facto* « présumée fiable » selon le décret n° 2001-272 et donc au sens de l'article 1316-4 du code civil[3]. Cette fiabilité entraîne, en cas de contentieux, le renversement de la charge de la preuve. Ce niveau de sécurité est de deux étoiles (**) – niveau élevé bien que non réputé « fiable » au sens du décret n° 2001-272 – pour les procès-verbaux et rapports signés par les personnes habilitées à constater des infractions, ainsi que pour les actes signés par les officiers de ministère public près les tribunaux de police et les juridictions de proximité.

2. La signature numérique

La signature numérique consiste en une signature manuscrite conservée sous forme numérique après avoir été apposée sur un écran tactile, au moyen d'un appareil sécurisé garantissant l'intégrité de

[2] Ce dispositif renvoie de fait à un procédé technique bien spécifique, qui est celui de la signature cryptographique. Pour une explication claire de ce procédé, voir sur le site du groupe Pérennisation des informations numériques (PIN), la présentation réalisée en 2009 par Frédéric Pailler (CNES) :
http://pin.association-aristote.fr/lib/exe/fetch.php/public/presentations/2009/pin20090113_cryptographie-pailler.pdf

[3] Article 2 du décret n°2001-272 : La fiabilité d'un procédé de signature électronique est présumée jusqu'à preuve contraire lorsque ce procédé met en œuvre une signature électronique sécurisée, établie grâce à un dispositif sécurisé de création de signature électronique et que la vérification de cette signature repose sur l'utilisation d'un certificat électronique qualifié ».
Voir le référentiel général de sécurité, partie 3.3.2 : http://www.ssi.gouv.fr/IMG/pdf/RGSv1-0.pdf
et annexe 8 : http://www.ssi.gouv.fr/IMG/pdf/RGS_PC-Type_Signature_V2-3.pdf

l'acte dès que la signature a été enregistrée. Celle-ci est apposée par les personnes concourant à la procédure et par les avocats ou toute autre personne amenée à signer les actes d'enquête ou d'instruction. Un certain nombre de précisions sont apportées concernant l'appareil sécurisé permettant cette signature numérique : niveau de résolution pour la saisie et pour la production de l'image, authentification de la personne, identification du signataire, garantie du lien entre la signature et l'acte auquel elle s'attache, intégrité de l'acte une fois la signature apposée. De la même façon que pour la signature électronique, une homologation de sécurité du système d'information est requise.

3. Les obligations en matière d'archivage

Le dispositif est sécurisé par l'introduction d'une obligation **d'archivage sécurisé** pour ces actes ainsi signés qui doivent alors être archivés dans un « système d'archivage électronique sécurisé ». Les fonctions de conservation, intégrité, intelligibilité, accessibilité et traçabilité durant la durée d'utilité courante et intermédiaire des documents sont requises, reprenant en cela la politique d'archivage dans le secteur public élaborée par l'ancienne direction centrale de la sécurité des systèmes d'information (actuelle agence nationale de la sécurité des systèmes d'information)[4]. Le format pérenne des documents est requis, de même que l'obligation de réplication des données sur un site distant, en conformité avec d'une part la norme ISO 14721 (norme OAIS de juin 2005[5]) et la norme Afnor Z 42-013 (version de mars 2009) sur l'archivage électronique.

D'ores et déjà ces dispositions se traduisent par deux projets menés d'une part par le ministère de la Justice et d'autre part le ministère de l'Intérieur, de l'Outre-mer, des Collectivités territoriales et de l'Immigration pour, respectivement, l'archivage sécurisé intermédiaire des minutes et ordonnances pénales contraventionnelles et des procès-verbaux de gendarmerie, projets auxquels sont étroitement associées les Archives de France.

Le directeur, chargé des Archives de France

Hervé LEMOINE

[4] http://www.ssi.gouv.fr/fr/bonnes-pratiques/outils-methodologiques/archivage-electronique-securise.html
[5] Voir la note d'information sur la norme OAIS en date du 8 juin 2011 sur le site des archives de France : http://www.archivesdefrance.culture.gouv.fr/static/4940