COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

La Convention 108 modernisée : aperçu des nouveautés

La version modernisée de la Convention 108 de 1981 réaffirme les principes d'origine de la Convention, en renforce certains et énonce quelques nouvelles garanties. Il a fallu adapter ces principes aux réalités du monde en ligne tandis que des pratiques inédites ont conduit à la reconnaissance de nouveaux principes. Les principes de transparence, de proportionnalité, de responsabilité, de limitation des données, de respect de la vie privée pris en compte dès la conception etc. sont désormais reconnus comme des éléments clés du mécanisme de protection et ont été intégrés dans l'instrument modernisé.

On peut présenter ainsi les principales nouveautés[1] de la Convention modernisée :

Objet et but de la Convention (article 1er)

L'article 1 souligne clairement l'objectif de la Convention, à savoir garantir à tout individu relevant de la juridiction de l'une des Parties (quels que soient sa nationalité et son lieu de résidence) la protection de ses données à caractère personnel lorsqu'elles sont soumises à un traitement, contribuant ainsi au respect de ses droits et de ses libertés fondamentales, et en particulier du droit à la vie privée.

Avec cette formulation, la Convention met en avant le fait que le traitement de données à caractère personnel peut permettre de manière positive l'exercice d'autres droits et libertés fondamentaux, facilité ainsi par la garantie du droit à la protection des données.

Définitions et champ d'application (articles 2 et 3)

Si les définitions de notions essentielles telles que « données à caractère personnel » et « personnes concernées » restent inchangées, des modifications ont été en revanche proposées pour d'autres définitions. Le concept de « fichier » est abandonné. Le terme « maître du fichier » est remplacé par « responsable du traitement », et les termes « sous-traitant » et « destinataire » ont été ajoutés.

Le champ d'application comprend à la fois le traitement automatisé et le traitement non automatisé des données à caractère personnel (traitement manuel où les données forment une structure permettant d'effectuer des recherches par personne concernée selon des critères prédéterminés), ce traitement relevant de la juridiction d'une Partie à la Convention. La portée générale de la Convention est conservée et son champ d'application continue naturellement de couvrir les traitements de données intervenant indistinctement dans les secteurs public et privé. Ceci est une des grandes forces de la Convention.

En revanche, la Convention ne s'applique plus au traitement de données effectué par une personne physique dans l'exercice d'activités purement personnelles ou domestiques.

[1] Le présent document expose les nouveautés et ne reprend pas les dispositions figurant déjà dans la Convention de 1981 et dans son protocole additionnel de 2001. Pour avoir une vue complète de la Convention modernisée, il convient de consulter la version consolidée, publiée sur notre site web.

En outre, les Parties n'ont plus la possibilité de procéder à des déclarations visant à les dispenser d'appliquer la Convention à certains types de traitements de données (par exemple à des fins de sécurité nationale et de défense).

Engagements des parties (article 4)

Chaque Partie est tenue d'adopter, dans son droit national, les mesures nécessaires pour donner effet aux dispositions de la Convention.

En outre, chaque Partie devra démontrer que de telles mesures ont été réellement engagées et ont pris effet. Elle devra également accepter que le Comité conventionnel vérifie que ces exigences sont respectées. Ce processus d'évaluation des Parties (« mécanisme de suivi ») est nécessaire pour garantir que les Parties offrent réellement le niveau de protection établi par la Convention.

Il est important de noter que les organisations internationales ont désormais la possibilité d'adhérer à la Convention (article 27), à l'exemple de l'Union européenne (article 26).

Légitimité du traitement de données et qualité des données (article 5)

L'article 5 précise l'application du principe de proportionnalité, soulignant qu'il doit s'appliquer tout au long du traitement, en particulier en ce qui concerne les moyens et les méthodes utilisés. Il est renforcé par ailleurs par le principe de limitation des données.

Une nouvelle disposition est introduite, énonçant précisément sur quel fondement juridique le traitement doit être effectué, à savoir le consentement de la personne concernée (qui doit répondre à plusieurs critères pour être valide) ou d'autres fondements légitimes prévus par la loi (contrat, intérêt vital de la personne concernée, obligation légale du responsable du traitement, etc.).

Données sensibles (article 6)

Le catalogue des données sensibles a été élargi et comprend désormais les données génétiques et biométriques ainsi que les données traitées pour les informations qu'elles révèlent sur l'appartenance syndicale ou l'origine ethnique (ces deux dernières catégories s'ajoutent aux données à caractère personnel faisant déjà l'objet d'une interdiction parce qu'elles révèlent l'origine raciale, les opinions politiques, les convictions religieuses ou autres convictions, la santé ou la vie sexuelle, et aux données à caractère personnel concernant des infractions et des procédures et condamnations pénales).

Sécurité des données (article 7)

S'agissant de la sécurité des données, l'obligation de notifier, sans retard, toute violation en matière de sécurité a été ajoutée. Cette exigence est limitée aux cas susceptibles de porter gravement atteinte aux droits et aux libertés fondamentales des personnes concernées ; ils doivent être notifiés, au moins, aux autorités de contrôle.

Transparence du traitement (article 8)

Les responsables du traitement seront tenus de garantir la transparence du traitement des données et devront fournir à cet effet une série d'informations concernant en particulier leur identité et leur lieu habituel de résidence ou d'établissement, la base juridique et les finalités du traitement, les destinataires des données et les catégories des données à caractère personnel traitées. Ils devront fournir par ailleurs toute information complémentaire nécessaire pour garantir un traitement loyal et transparent. Le responsable du traitement n'est pas tenu de fournir ces informations dès lors que le traitement est expressément prévu par la loi ou que cela s'avère impossible ou implique des efforts disproportionnés.

Droits des personnes concernées (article 9)

De nouveaux droits sont octroyés aux personnes concernées pour qu'elles puissent davantage contrôler leurs données à l'ère numérique.

La Convention modernisée élargit le catalogue des informations devant être transmises aux personnes concernées lorsqu'elles exercent leur droit d'accès. Ces personnes ont par ailleurs le droit d'obtenir connaissance du raisonnement qui sous-tend le traitement de données, lorsque les résultats de ce traitement sont appliqués. Ce nouveau droit leur est particulièrement important pour le profilage d'individus[2].

Il convient d'associer ce droit à une autre nouveauté, à savoir le droit de la personne concernée de ne pas être soumise à une décision l'affectant qui serait fondée uniquement sur un traitement automatisé, sans que son point de vue soit pris en compte.

Les personnes concernées ont le droit de s'opposer à tout moment au traitement de leurs données à caractère personnel, à moins que le responsable du traitement ne démontre des motifs légitimes justifiant le traitement qui prévalent sur les intérêts ou sur les droits et les libertés fondamentales.

Obligations complémentaires (article 10)

La Convention modernisée impose des obligations plus vastes aux personnes traitant les données ou ayant confié le traitement des données à d'autres personnes en leur nom.

La notion de responsabilité fait désormais partie intégrante du système de protection, avec l'obligation pour les responsables du traitement d'être en mesure de démontrer qu'ils respectent les règles relatives à la protection des données.

Les responsables du traitement doivent prendre toutes les mesures appropriées - (y compris lorsque le traitement est sous-traité) - afin de veiller à ce que le droit à la protection des données soit assuré (respect de la vie privée dès la conception, examen de l'impact potentiel du traitement de données envisagé sur les droits et les libertés fondamentales des personnes concernées (« évaluation de l'impact sur le respect de la vie privée ») et respect de la vie privée par défaut).

Exceptions et restrictions (article 11)

Les droits énoncés dans la Convention ne sont pas absolus et peuvent être limités lorsque ceci est prévu par la loi et constitue une mesure nécessaire dans une société démocratique sur la base de motifs spécifiés et limités. Ces motifs limités comprennent désormais des « objectifs essentiels d'intérêt public » ainsi qu'une référence au droit à la liberté d'expression.

Quelques éléments ont été ajoutés à la liste des dispositions de la Convention pouvant être restreintes (voir les références à l'article 7 paragraphe 1 sur la sécurité et à l'article 8 paragraphe 1 sur la transparence sous l'article 11 paragraphe 1). Cet article comporte un nouveau paragraphe portant spécifiquement sur les activités de traitement à des fins de sécurité nationale et de défense, où il est indiqué que les pouvoirs de « surveillance » du Comité ainsi que certianes missions des autorités de contrôle peuvent être limités. Il est clairement énoncé que les activités de traitement à des fins de sécurité nationale et de défense doivent faire l'objet d'un contrôle et d'une supervision indépendants et effectifs.

Il est important de rappeler une fois de plus que, contrairement aux précédentes dispositions de la Convention 108, les Parties à la Convention modernisée ne pourront plus exclure certains types de traitement du champ d'application de la Convention.

[2] Voir à ce sujet la Recommandation (2010) 13 sur la protection des personnes à l'égard du traitement automatisé des données à caractère personnel dans le cadre du profilage, ainsi que l'exposé des motifs.

Flux transfrontières de données à caractère personnel (article 14)

Cette disposition a pour objet de faciliter, s'il y a lieu, la libre circulation d'informations par-delà les frontières tout en assurant une protection adéquate aux individus en ce qui concerne le traitement des données à caractère personnel.

Le but du système de flux transfrontières est de garantir que les informations traitées à l'origine dans la juridiction d'une Partie demeurent toujours protégées par des principes appropriés de protection des données.

Les flux de données entre les Parties ne peuvent pas être interdits ni soumis à une autorisation spéciale car toutes les Parties, qui ont souscrit à la base commune de dispositions sur la protection des données énoncées dans la Convention, offrent le niveau de protection jugé approprié. Il existe néanmoins une exception, lorsqu'il existe un risque réel et sérieux que ce transfert de données conduise à contourner les dispositions de la Convention.

En l'absence de règles de protection harmonisées et communes à des États appartenant à une organisation internationale régionale et gérant les flux de données (par exemple le cadre de protection des données de l'Union européenne), les données devraient circuler librement entre les Parties.

En ce qui concerne les flux transfrontières de données vers un destinataire ne relevant pas de la juridiction d'une Partie, un niveau approprié de protection doit être garanti dans l'État ou l'organisation où se trouve le destinataire. Ceci ne pouvant pas être présupposé puisque le destinataire n'est pas Partie à la Convention, deux principaux moyens sont prévus pour veiller à ce que le niveau de protection des données soit bien approprié : soit la règle de droit, soit des garanties ad hoc ou standardisées agréées, établies par des instruments juridiquement contraignants et opposables (notamment des clauses contractuelles ou des règles générales contraignantes) et correctement mises en œuvre.

Autorités de contrôle (article 15)

S'appuyant sur l'article 1er du protocole additionnel, la Convention modernisée ajoute une disposition au catalogue des pouvoirs des autorités de contrôle. Outre leurs pouvoirs d'intervention, d'investigation, d'ester en justice ou de porter à la connaissance des autorités judiciaires des violations des dispositions relatives à la protection des données, les autorités sont chargées également de sensibiliser le public, de fournir des renseignements et d'informer tous les acteurs concernés (personnes concernées, responsables du traitement, sous-traitants, etc.). Elles peuvent également prendre des décisions et imposer des sanctions. Il est rappelé par ailleurs que les autorités de contrôle doivent exercer ces tâches et ces pouvoirs en toute indépendance.

Formes de coopération (article 17)

La Convention modernisée porte également sur la question de la coopération (et de l'assistance mutuelle) entre les autorités de contrôle.

Les autorités de contrôle doivent coordonner leurs investigations, mener des actions conjointes et se fournir mutuellement des informations et des documents sur leur droit et leurs pratiques administratives en matière de protection des données.

Les informations ainsi échangées ne comprendront des données à caractère personnel que si ces données sont essentielles à la coopération ou si la personne concernée a donné un consentement spécifique, libre et éclairé pour ce faire.

Enfin, la Convention prévoit un forum pour renforcer la coopération : les autorités de contrôle des Parties doivent se constituer en réseau afin d'organiser leur coopération et d'accomplir leurs fonctions comme le prévoit la Convention.

Comité conventionnel (articles 22, 23 et 24)

Le Comité conventionnel joue un rôle crucial pour l'interprétation de la Convention en encourageant l'échange d'informations entre les Parties et le développement de normes sur la protection des données.

La Convention modernisée renforce le rôle et les pouvoirs du Comité qui n'a plus seulement un rôle « consultatif » mais se voit également conférer des pouvoirs d'évaluation et de surveillance. Il formulera un avis sur le niveau de protection des données assuré par un État ou une organisation internationale préalablement à leur adhésion à la Convention. Il peut aussi évaluer si le droit interne de la Partie concernée est conforme aux dispositions de la Convention et déterminer si les mesures prises ont été suivies d'effet (existence d'une autorité de contrôle, responsabilités, existence de voies de recours en vigueur).

Le Comité peut également évaluer si les normes légales régissant les transferts de données garantissent de manière suffisante un niveau approprié de protection des données.