7 mai 2021 T-PD(2020)06rev3

COMITÉ CONSULTATIF DE LA CONVENTION POUR LA PROTECTION DES PERSONNES À L'ÉGARD DU TRAITEMENT AUTOMATISÉ DES DONNÉES À CARACTÈRE PERSONNEL

CONVENTION 108

INTERPRÉTATION DES DISPOSITIONS[1]

Direction Générale – Droits de l'Homme et État de droit

[1] Le présent avis du Comité de la Convention 108 contient des orientations visant à faciliter la ratification du protocole d'amendement à la Convention

Le présent document vise à répondre à la demande formulée par une délégation lors de la 39e réunion plénière (19-21 novembre 2019) du Comité de la Convention 108, complétée par une demande supplémentaire lors de la 50e réunion du Bureau du Comité (28-30 septembre 2020).

Voir les paragraphes :

- 2.16 du rapport abrégé de la 39e réunion plénière demandant l'interprétation des termes « traitement arithmétique » (article 2, définition du « traitement des données) », la distinction faite entre le statut juridique du « responsable de traitement » et du « destinataire », et pour des orientations sur l'anonymisation et la pseudonymisation, en relation avec une « personne identifiée ou identifiable » ; et

- 2.14 du rapport abrégé de la 50e réunion du Bureau demandant clarification des notions de « divulgation » et de flux transfrontières de données.
L'interprétation des concepts a un caractère d'orientation et vise à aider les États parties à la Convention 108 à ratifier le Protocole d'amendement à la Convention 108.

1) <u>« Opérations arithmétiques » (article 2.b de la Convention 108+)</u>

« Traitement de données » s'entend de toute opération ou ensemble d'opérations effectuées sur des données à caractère personnel, telles que la collecte, l'enregistrement, la conservation, la modification, l'extraction, la communication, la mise à disposition, l'effacement ou la destruction des données, ou l'application **d'opérations** logiques et/ou **arithmétiques** à ces données.

(La Convention 108 comporte une formulation similaire.)

Les termes « arithmétique et/ou logique » font référence à l'une des composantes de base d'un processeur informatique, appelée unité arithmétique et logique (UAL).

L'UAL est un circuit numérique combinatoire qui effectue des opérations arithmétiques et logiques sur des nombres binaires entiers. Il s'agit d'un élément fondamental de nombreux types de circuits informatiques, y compris de l'unité centrale de traitement (UC) des ordinateurs.

Les opérations arithmétiques sont effectuées à partir de données d'entrée (*data input*) et les résultats désignés sous le terme de sortie (*output*).

2) <u>Distinction entre le statut juridique du « responsable du traitement » et du « destinataire »</u>

Les définitions de « responsable du traitement » et de « destinataire » au sens de la Convention 108+ sont les suivantes :

d. « responsable du traitement » désigne la personne physique ou morale, l'autorité publique, le service, l'agence ou tout autre organisme qui, seul ou conjointement avec d'autres, dispose du pouvoir de décision à l'égard du traitement de données ;

e. « destinataire » désigne la personne physique ou morale, l'autorité publique, le service, l'agence ou tout autre organisme qui reçoit communication de données ou à qui des données sont rendues accessibles.

Selon le paragraphe 22 du rapport explicatif de la Convention 108+, « responsable du traitement » désigne la personne ou l'organe qui dispose du pouvoir de décision à l'égard des finalités et moyens du traitement de données, que ce soit en vertu d'une désignation officielle ou de circonstances factuelles à apprécier au cas par cas. Il peut y avoir plusieurs responsables ou co-responsables du traitement (conjointement responsables d'un traitement ou en charge de différents aspects d'un traitement). Afin de déterminer si un organe ou une personne peuvent être qualifiés de responsable du traitement, une attention particulière doit être portée au fait de savoir si il ou elle détermine les motifs justifiant le traitement, à savoir ses finalités, ainsi que les moyens utilisés. D'autres facteurs pertinents dans cet exercice de qualification comprennent le fait de contrôler ou non les méthodes du traitement, le choix des données à traiter et les personnes autorisées à y accéder. Les personnes qui ne sont pas directement subordonnées au responsable du traitement et qui effectuent le traitement pour son compte, conformément à ses instructions, sont des sous-traitants. Le responsable du traitement conserve la responsabilité du traitement lorsque ce dernier est effectué pour son compte par un sous-traitant.

Le paragraphe 24 du rapport explicatif prévoit que le « sous-traitant » est toute personne physique ou morale (autre que les employés du responsable du traitement) qui accomplit les opérations de traitement pour le compte du responsable du traitement conformément à ses instructions, lesquelles définissent les limites de l'utilisation autorisée des données à caractère personnel par le sous-traitant.

Le paragraphe 23 du rapport explicatif stipule que le « Destinataire » désigne la personne ou l'entité qui reçoit des données à caractère personnel ou à qui ces données sont rendues accessibles. Selon le cas, le destinataire peut être un responsable du traitement ou un sous-traitant. Par exemple, une entreprise peut envoyer certaines données de ses employés au ministère compétent, qui les traitera à des fins fiscales en tant que responsable du traitement. Elle peut les envoyer à une société proposant des services de stockage, celle-ci jouant alors le rôle de sous-traitant. Le destinataire peut être un organisme public ou une entité qui se sont vus reconnaître le droit d'exercer une fonction publique mais lorsque les données reçues par cet organisme ou entité sont traitées dans le cadre d'une demande particulière conformément au droit applicable, cet organisme ou entité ne seront pas considérés comme un destinataire. Les demandes de communication faites par les autorités publiques devraient toujours être présentées par écrit, être motivées et revêtir un caractère occasionnel, et elles ne devraient pas porter sur l'intégralité d'un fichier ni conduire à l'interconnexion de fichiers. Le traitement des données à caractère personnel par les autorités publiques en question devrait être effectué dans le respect des règles applicables en matière de protection des données en fonction des finalités du traitement.

Le terme « destinataire » est donc utilisé pour désigner les « responsables du traitement » ou les « sous-traitants », selon le cas, auxquels des données à caractère personnel sont communiquées ou mises à disposition, sans aucune précision quant à leur relation ou leur statut juridique dans la chaîne du traitement (c'est-à-dire en tant que responsable du traitement ou sous-traitant). Et tant que telle, la personne ou l'entité juridique à laquelle il est fait référence peut être soit un « responsable du traitement », soit un « sous-traitant » en fonction de ses opérations de traitement de données. Par conséquent, le terme « destinataire » ne peut pas être considéré comme un statut juridique (assorti de droits et de devoirs) mais comme décrivant une situation dans laquelle un niveau supplémentaire dans la relation entre la personne concernée et les responsables du traitement et les sous-traitants est ajouté par le ou les opérations du responsable du traitement initial.

Il convient néanmoins de noter qu'en ce qui concerne l'article 8.1.d de la Convention 108+ , le responsable du traitement doit informer les personnes concernées - entre autres – « des destinataires ou catégories de destinataires des données à caractère personnel ». De plus, conformément à l'article 14.2 de la Convention 108+, un État partie doit veiller à ce qu'un « niveau approprié de protection fondé sur les dispositions de la présente Convention soit garanti » par et pour tous les destinataires d'un pays ou d'une organisation non-partie au Protocole d'amendement STCE 223, quels que soient leur statut juridique et leur relation (c'est-à-dire responsable du traitement ou sous-traitant, ou autre statut) au titre de leur législation nationale.

Exemples concrets : responsable du traitement / sous-traitant / destinataire

- Une université est engagée par le gouvernement pour un projet de recherche sur le développement économique de la population. Les données personnelles pertinentes seront fournies par le gouvernement qui déterminera également les finalités et les principaux moyens du traitement. Même si l'université a toute latitude, et donc dispose d'une certaine marge de manœuvre pour définir la manière dont la recherche sera effectuée en termes de méthodologie, elle ne recueillera aucune donnée personnelle, la recherche sera effectuée par le biais de la base de données fournie par le gouvernement.

    - Dans ce cas, l'université est le sous-traitant et le gouvernement le responsable du traitement.

- Pour améliorer la sécurité de ses élèves, une école prévoit d'engager une entreprise de sécurité pour contrôler l'accès à l'école. L'entreprise sera chargée de fournir des caméras ainsi que des badges électroniques aux étudiants.

  La collecte des données personnelles est effectuée par l'école, et l'école partage avec l'entreprise les données personnelles qui seront utilisées pour autoriser l'accès aux élèves.

  À aucun moment l'entreprise ne définit les données qui seront collectées ; elle ne reçoit de l'école que les données nécessaires pour autoriser l'accès des élèves à l'école.

    - L'école est le responsable du traitement et l'entreprise est le sous-traitant.

- Une organisation internationale de défense des droits de l'homme prévoit d'effectuer une mission dans un camp de réfugiés. Il est nécessaire de collecter différents types de données personnelles pour comprendre les circonstances des réfugiés et pour leur fournir des médicaments, de la nourriture, des vêtements, etc.

  Pour cette mission, l'organisation internationale décide d'engager une société pour stocker les données et une autre pour les compiler et fournir des statistiques sur le type et la quantité de médicaments nécessaires pour tous les réfugiés.

    - L'organisation internationale est le responsable du traitement et les deux autres sociétés les sous-traitants.

- Un employé d'une entreprise privée procède à une évaluation régulière de passeports et autres données personnelles pour déterminer s'il est possible de laisser entrer des personnes dans un pays.

L'employé doit partager ces informations avec un système gouvernemental afin de vérifier que les personnes ne sont pas des délinquants ou ne font pas l'objet d'une interdiction de quitter le territoire pour motifs sécuritaires.

- Dans ce cas, le gouvernement est le destinataire agissant comme responsable du traitement distinct et l'employé est le sous-traitant au nom de l'entreprise chargée par contrat des services d'évaluation.

- La société Alpha est soumise à des obligations fiscales et partage les données relatives aux salaires avec les autorités publiques à des fins fiscales.

  - Dans ce cas, l'autorité publique est le destinataire (comme responsable du traitement distinct en ce qui concerne ses propres traitements après avoir reçu les données) et la société est le responsable du traitement.

Un service de nuage informatique (« cloud ») est fourni par une entreprise (A) pour le traitement des données personnelles liées aux ressources humaines d'une autre entreprise (B). L'entreprise (A) fournissant les services cloud doit informer l'entreprise requérante (B) de tous ses partenaires auxquels elle transférera des données dans le cadre de l'exécution du contrat de service de nuage informatique.

- La société (B) qui demande les services de nuage informatique est le responsable du traitement des données, la société (A) qui fournit les services de nuage informatique est le sous-traitant tandis que ses partenaires commerciaux sont les destinataires.

3) <u>« Personne identifiée ou identifiable » – orientation ou collecte de bonnes pratiques sur le processus d'anonymisation et de pseudonymisation</u>

Le paragraphe 18 du rapport explicatif de la Convention 108+ se lit comme suit : *« Le terme 'identifiable' ne fait pas uniquement référence à l'identité civile ou juridique de la personne en tant que telle, mais également à tout élément susceptible d' « individualiser » ou de distinguer (et donc de traiter différemment) une personne parmi d'autres. Cette « individualisation » pourrait se faire, par exemple, à partir d'un numéro d'identification, d'un pseudonyme, de données biométriques ou génétiques, de données de localisation, d'une adresse IP ou d'un autre identifiant, qui renvoient à une personne donnée ou à un dispositif ou un ensemble de dispositifs (ordinateur, téléphone portable, appareil photo, console de jeu, etc. L'utilisation d'un pseudonyme ou de tout identifiant/identité numérique n'entraîne pas l'anonymisation des données, la personne concernée pouvant encore être identifiable ou individualisée. Les données pseudonymisées doivent donc être considérées comme des données à caractère personnel et sont à ce titre couvertes par les dispositions de la Convention. La qualité des techniques de pseudonymisation appliquées lors du traitement des données devrait être dûment prise en compte lors de l'évaluation de la pertinence des garanties mises en place afin de réduire les risques pour les personnes concernées. »*

Le paragraphe 19 du rapport explicatif de la Convention 108+ fournit que « *Les données ne peuvent être considérées comme anonymes que lorsque la ré-identification de la personne concernée est impossible ou nécessiterait des délais, efforts ou ressources déraisonnables, au vu des technologies disponibles au moment du traitement et de l'évolution de celles-ci. Des données en apparence anonymes car non assorties d'un élément d'identification évident peuvent néanmoins, dans certains cas (ne nécessitant pas des délais, activités ou ressources déraisonnables), permettre l'identification d'une personne. C'est notamment le cas lorsque la combinaison de différents types de données, telles que des données physiques, physiologiques, génétiques, économiques ou sociales (combinaison de données relatives à l'âge, le sexe, l'activité professionnelle, la géolocalisation, la situation de famille, etc.) permettent au responsable du traitement, ou à toute autre personne, d'identifier la personne concernée. Dans pareille situation, les données ne sauraient être considérées comme anonymes et sont couvertes par les dispositions de la Convention.* »

Le paragraphe 19 du rapport explicatif de la Convention 108+ prévoit que « *Lorsque des données sont rendues anonymes, des moyens appropriés doivent être mis en place pour empêcher toute ré-identification des personnes concernées ; en particulier, tous les moyens techniques doivent être mis en œuvre pour garantir que la personne n'est plus identifiable. Vu la rapidité des évolutions techniques, ces moyens techniques devraient être réévalués régulièrement*. »

Il découle de ce qui précède que l'anonymisation des données à caractère personnel pourrait être obtenue non seulement par un processus qui résulterait dans une impossibilité de réidentification de la personne concernée, mais également, si le processus conduisait à des données à travers lesquelles la réidentification d'un individu exigerait « *des délais, efforts ou ressources déraisonnable au vu des technologies disponibles au moment du traitement et de l'évolution de celles-ci* ». Étant donné que la technologie évolue rapidement et que les circonstances et le contexte peuvent varier considérablement, il ne semble pas souhaitable de décrire en termes et de chiffres concrets ce qui devrait constituer « des délais, efforts ou ressources déraisonnables », ni de donner des exemples d'une telle situation. Se basant sur le principe selon lequel un responsable du traitement est responsable du traitement qu'il effectue avec des données personnelles, il serait de sa responsabilité de catégoriser les données personnelles et non personnelles (c'est-à-dire anonymisées) avant de lancer le traitement. En cas de doute, car cela pourrait être d'une importance fondamentale, l'autorité de contrôle pourrait indiquer sur une donnée ou un ensemble de données s' ils sont convenablement anonymisés ou non. Elle le ferait cependant sans préjudice de la responsabilité du responsable du traitement si les données ou l'ensemble de données en question pouvaient être utilisées pour identifier à nouveau des personnes (par une nouvelle technologie, technique, un responsable du traitement conjoint, etc.).

Dans un effort d'harmonisation des pratiques de procédures d'anonymisation, les autorités nationales de contrôle sont encouragées à publier des lignes directrices et des recommandations[2].

[2] Pour plus d'information sur l'anonymisation et la pseudonymisation, voir :
Avis 05/2014 sur les Techniques d'anonymisation adopté par le groupe de travail « Article 29 » sur la protection des données : https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm
Document commun du Contrôleur européen de la protection des données (CEPD) et de l'Agencia española de protección de datos (AEPD) : « Introduction à la fonction de hachage en tant que technique de pseudonymisation des données personnelles » concernant l'anonymisation : https://edps.europa.eu/data-protection/our-work/publications/papers/introduction-hash-function-personal-data_en
Guide sur l'anonymisation et la pseudonymisation par l'APD (autorité de protection des données) irlandaise, juin 2019 : https://www.dataprotection.ie/en/guidance-landing/anonymisation-and-pseudonymisation

4) Communication / divulgation

Les références à la communication / divulgation de données dans la Convention 108+ sont les suivantes :

Dans l'article 2b : « traitement de données » s'entend de toute opération ou ensemble d'opérations effectuées sur des données à caractère personnel, telles que (…) **communication** (…).

Dans l'article 2e : « destinataire » signifie : la personne physique ou morale, l'autorité publique, le service, l'agence ou tout autre organisme qui reçoit **communication** de données ou à qui des données sont rendues accessibles.

Dans l'article 7.1 : « *Chaque Partie prévoit que le responsable du traitement, ainsi que le cas échéant le sous-traitant, prend des mesures de sécurité appropriées contre les risques tels que l'accès accidentel ou non autorisé aux données à caractère personnel, leur destruction, perte, utilisation, modification ou* ***divulgation*** ».

De plus, le rapport explicatif de la Convention 108+ fait également référence à la communication de données dans les paragraphes suivants :

paragraphe 23 : « …***divulgation*** *par les autorités publiques…* »
paragraphe 64 : « … *la* ***révélation*** *de données couvertes par le secret professionnel…* »
paragraphe 102 : « *Un transfert transfrontière de données intervient lorsque des données à caractère personnel sont* ***communiquées*** *ou mises à disposition d'un destinataire relevant de la juridiction d'un autre État ou d'une autre organisation*. »

Sur la base de ce qui précède, on entend par « communication » une opération de traitement des données effectuée par le responsable du traitement, qui consiste à faire connaître les données à caractère personnel au grand public ou à un destinataire.

L'autre signification de ce terme se rapporte aux actions effectuées par le responsable du traitement telles que l'envoi, la divulgation ou l'octroi d'un accès à des données à caractère personnel. Dans ce sens, le paragraphe 23 du rapport explicatif donne l'exemple d'une « demande de communication » par une autorité publique qui fait référence à une demande officielle d'accès faite par une autorité publique à des données détenues dans une base de données privée.

En général, son utilisation en tant que définition distincte dépendra de la logique de la législation nationale. À cet égard, les éventuelles exigences constitutionnelles selon lesquelles les données personnelles ne peuvent être divulguées que si la loi le prévoit doivent être prises en compte. (Par exemple, les autorités publiques ne peuvent pas divulguer des données personnelles dans une situation donnée sans y être autorisées par la loi. Dans ces situations, la loi stipulera tous les destinataires et les finalités d'une telle divulgation).

Anonymisation : code de pratique pour la gestion des risques liés à la protection des données par l'OIC : https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwipk7GSrK_sAhXLDuwKHb4wDUUQFjAAegQIAhAC&url=https%3A%2F%2Fico.org.uk%2Fmedia%2F1061%2Fanonymisation-code.pdf&usg=AOvVaw3e_7fB2B38Tfpyx66OXh9s
Lignes Directrices de l'autorité de contrôle de l'Uruguay (en espagnol) : https://www.gub.uy/unidad-reguladora-control-datos-personales/comunicacion/publicaciones/guia-criterios-disociacion-datos-personales/guia-criterios-disociacion

Le paragraphe 23 rappelle que la communication doit respecter les règles applicables en matière de protection des données, notamment en ce qui concerne la forme de la demande, la proportionnalité, la nécessité et la finalité du traitement.

5) Flux transfrontières de données

L'article 14 de la Convention 108+ est libellé comme suit :

1. Une Partie ne peut, aux seules fins de la protection des données à caractère personnel, interdire ou soumettre à une autorisation spéciale le transfert de ces données à un destinataire relevant de la juridiction d'une autre Partie à la Convention. Cette Partie peut néanmoins agir ainsi lorsqu'il existe un risque réel et sérieux que le transfert à une autre Partie, ou de cette autre Partie à une non-Partie, conduise à contourner les dispositions de la Convention. Une Partie peut également agir ainsi lorsqu'elle est tenue de respecter des règles de protection harmonisées communes à des États appartenant à une organisation internationale régionale.

2. Lorsque le destinataire relève de la juridiction d'un État ou d'une organisation internationale qui n'est pas Partie à la présente Convention, le transfert de données à caractère personnel n'est possible que si un niveau approprié de protection fondé sur les dispositions de la présente Convention est garanti. »

Rapport explicatif :

102. (…) Un transfert transfrontière de données intervient lorsque des données à caractère personnel sont communiquées ou mises à disposition d'un destinataire relevant de la juridiction d'un autre État ou d'une autre organisation internationale.

103. Le régime des flux transfrontières vise à garantir que des données à caractère personnel traitées à l'origine dans la juridiction d'une Partie (données collectées ou conservées dans cette juridiction, par exemple), qui relèvent ensuite de la juridiction d'un État non-partie à la Convention continuent d'être traitées avec des garanties appropriées. L'important est que les données traitées dans la juridiction d'une Partie soient toujours protégées par les principes pertinents de la Convention. (…)

104. L'article 14 s'applique à l'exportation de données et non pas à leur importation, dans la mesure où dans ce dernier cas, les données relèvent alors du régime de protection des données de la Partie destinataire. »

L'article 14 de la Convention 108+, qui prévoit le régime de flux transfrontières, s'applique lorsque des données à caractère personnel sont transférées hors de la juridiction d'une Partie (vers une autre Partie, qu'il s'agisse d'un État ou d'une organisation internationale, ou vers un État ou une organisation internationale non-Partie à la Convention). Alors que toutes les données personnelles « relevant de la juridiction» d'une Partie (article 3) devraient bénéficier des protections prévues par la Convention 108+, il convient de noter que l'article 14 s'applique spécifiquement aux exportations de données plutôt qu'aux importations.
En ce qui concerne cette notion de « juridiction », l'avis juridique fournit par le Conseiller juridique (DLAPIL02/2021_JP/DG[3], « Avis juridique ») peut être pertinent.

[3] https://rm.coe.int/legal-opinion-dlapil02-2021-the-interpretation-of-the-notion-of-jurisd/1680a19c58 (en anglais uniquement)

Compte tenu de l'applicabilité de la Convention 108+ et en particulier des articles 3 et 14, le terme juridiction, en plus de la règle de territorialité, devrait être interprété comme englobant « *toutes les situations dans lesquelles une partie a le pouvoir juridique de légiférer et de mettre en œuvre effectivement les règles relatives aux traitements des données personnelles* », conformément au paragraphe 35 de l'avis juridique. Ce faisant, les Parties peuvent envisager, au moment de l'adoption de la législation et lors de la mise en œuvre de la Convention 108+, la coopération des autorités de contrôle, comme décrit à l'article 17, fournissant un outil unique pour la mise en application collective des droits protégés par la Convention 108+ et pour la facilitation de la libre circulation des données entre Parties.