N° 297

ASSEMBLÉE NATIONALE

CONSTITUTION DU 4 OCTOBRE 1958

SEIZIÈME LÉGISLATURE

Enregistré à la Présidence de l'Assemblée nationale le 11 octobre 2022.

RAPPORT

FAIT

AU NOM DE LA COMMISSION DES AFFAIRES ÉTRANGÈRES SUR LE PROJET DE LOI, ADOPTÉ PAR LE SÉNAT, *autorisant la* **ratification** *du* **Protocole** *d'***amendement** *à la* **Convention** *pour la* **protection** *des* **personnes** *à l'***égard** *du* **traitement** *automatisé des* **données** *à* **caractère personnel**,

PAR MME ERSILIA SOUDAIS
Députée

ET

ANNEXE : TEXTE DE LA COMMISSION DES AFFAIRES ÉTRANGÈRES

Voir les numéros :

Assemblée nationale : **5.**

Sénat : **561, 749, 750** et T.A. **138** (2020-2021).

SOMMAIRE

Pages

INTRODUCTION

La commission des affaires étrangères est saisie du projet de loi n° 5 autorisant la ratification du protocole d'amendement à la convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, conséquemment à son adoption par le Sénat le 13 juillet 2021.

Le protocole d'amendement, dit « protocole 223 », signé par la France le 10 octobre 2018, vient apporter des modifications à la convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, dite n° 108, signée par la France le 28 janvier 1981. Il poursuit un double objectif de modernisation en réponse, d'une part, aux évolutions technologiques associées à l'utilisation de nouvelles technologies de l'information et de la communication et, d'autre part, à l'intensification des échanges de données personnelles à l'échelle internationale. Cela s'est vérifié par exemple dans des cadres de coopérations récemment comme au niveau des données de santé et de paramètres biométriques pour les mouvements transfrontaliers post-COVID, mais également dans des scandales venant des opérateurs américains suite à l'affaire Facebook / Cambridge Analytica, et sur des exemples de croisements et transferts de données entre plateformes en France avec la Caisse d'allocations familiales (CAF), qui a utilisé ces données pour réaliser des profilages des allocataires sur la base de données sensibles et pour ficher des « profils à risque de fraude ». Récemment, des ONG ont lancé une pétition contre Doctolib pour dénoncer l'envoi direct de données sensibles aux États-Unis sans anonymisation préalable, ce qui est contraire au Règlement général sur la protection des données (RGPD).

Si l'entrée en vigueur du protocole viendra consolider l'édifice juridique européen et international existant en matière de protection des données personnelles, elle doit également s'accompagner d'une attention renouvelée et accrue aux acteurs appelés à assurer la mise en œuvre des règles de droit encadrant le secteur du numérique, tout particulièrement les acteurs publics qui ne bénéficient pas de moyens équivalents à ceux des grandes entreprises du secteur.

En effet, il s'agit d'un domaine qui a fait l'objet d'une adaptation juridique dense et dynamique ces dernières années, entraînant pour les acteurs concernés – qu'ils soient spécialistes ou généralistes – des conséquences pratiques substantielles, auxquelles il n'est pas toujours évident de faire face.

I. LE PROTOCOLE 223 VIENT MODERNISER ET RENFORCER UN INSTRUMENT JURIDIQUE INTERNATIONAL UNIQUE DÉDIÉ À LA PROTECTION DES DONNÉES PERSONNELLES

A. UN TEXTE DE RÉFÉRENCE POUR LA PROTECTION DES DONNÉES PERSONNELLES

Le « protocole 223 » apporte des modifications et des compléments à la convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, dite « convention 108 ». Cette dernière, datant de 1981, est le premier instrument international juridique contraignant à être entré en vigueur dans ce domaine et demeure le seul à ce jour. La France a signé la convention dès le jour de son ouverture à la signature, le 28 janvier 1981. Elle l'a ratifiée le 24 mars 1983.

La convention 108 est entrée en vigueur le 1er octobre 1985. Elle compte aujourd'hui cinquante-cinq États parties, ce qui inclut les quarante-six États membres du Conseil de l'Europe, auxquels s'ajoutent neuf États tiers (1). En effet, la portée de cette convention dépasse le cadre régional du Conseil de l'Europe et de ses États membres.

La convention de 1981 a pour principal objectif de protéger la vie privée des personnes physiques à l'égard des traitements automatisés des données à caractère personnel qui les concernent et ce sur le territoire de chaque État partie, quelle que soit la nationalité des personnes. Selon la convention 108, les données à caractère personnel désignent « *toute information concernant une personne physique identifiée ou identifiable* » et le traitement de données s'entend de « *toute opération ou ensemble d'opérations effectuées sur des données à caractère personnel* », telles que la collecte, la communication, la modification ou encore l'effacement de données.

Le 8 novembre 2001, un premier protocole additionnel concernant les autorités de contrôle et les flux transfrontières de données a été ouvert à la signature. Il impose notamment la mise en place d'autorités de contrôle indépendantes chargées d'assurer le respect des règles nationales résultant de la convention. La France a signé ce protocole en 2001 et l'a ratifié le 22 mai 2007, soit après son entrée en vigueur en 2004. Il compte à ce jour quarante-quatre États parties, dont les neuf États non-membres du Conseil de l'Europe qui sont parties à la convention de 1981.

Si la convention 108 et son protocole additionnel constituent un ensemble juridique unique au monde en matière de protection des données personnelles, ils sont complétés par d'autres outils qui n'y sont pas exclusivement consacrés mais y contribuent.

---

(1) Argentine, Cap Vert, Maroc, Maurice, Mexique, Sénégal, Tunisie, Uruguay et, depuis 2022, Russie (suite à son exclusion du Conseil de l'Europe après le déclenchement de son offensive contre l'Ukraine).

Ainsi, la convention européenne de sauvegarde des droits de l'Homme et des libertés fondamentales du 4 novembre 1950 ne comporte pas de dispositions spécifiques sur les données personnelles mais elle permet d'encadrer les traitements de telles données, principalement par l'application que fait la Cour européenne des droits de l'homme (CEDH) des stipulations de son article 8, qui garantit notamment le droit au respect de la vie privée.

On peut également citer la convention de Budapest sur la cybercriminalité du 23 novembre 2001, qui fait référence à la convention 108 dans son préambule. En outre, la négociation récente d'un second protocole additionnel à cette convention a inclus des discussions sur l'intégration de références plus directes à la protection des données, visant à clarifier et renforcer le régime applicable aux accès de données transfrontières. Le texte prévoit notamment (article 14 dédié à la protection des données personnelles), que la « convention 108 + » (ensemble désignant la convention de 1981 avec le protocole 223) ou d'autres accords internationaux globaux en matière de protection des données s'appliqueraient par priorité sur les dispositions du protocole additionnel à la convention de Budapest relatives aux protections des données, dès lors que les Parties concernées en seraient Parties et sauf accord contraire des Parties (1).

B. UN PROTOCOLE QUI VIENT S'INSÉRER DANS LE DROIT EUROPÉEN ET LE DROIT NATIONAL

1. Un renforcement du positionnement européen en matière de protection des données personnelles

Si le protocole 223 est un instrument de droit international unique en son genre, la protection juridique des données personnelles se joue également au niveau européen. En effet, l'Union européenne apparaît aujourd'hui comme une référence au plan mondial en matière de protection des données personnelles.

Dans l'ensemble, l'articulation entre les stipulations du protocole additionnel et la nouvelle convention 108 +, d'une part, et le droit européen, d'autre part, ne soulève pas de difficultés.

Le droit à la protection des données à caractère personnel est consacré par le droit primaire, en particulier par l'article 16 du traité sur le fonctionnement de l'Union européenne (TFUE) et l'article 8 de la Charte des droits fondamentaux de l'Union européenne. Il est par ailleurs protégé par des normes de droit dérivé, à commencer par le Règlement général sur la protection des données (règlement 2016/679 du 27 avril 2016) dit « RGPD » et par la directive dite « Police – Justice » (directive 2016/680 du 27 avril 2016) (2).

---

(1) Le protocole a été ouvert à la signature le 12 mai 2022 et a depuis été signé par vingt-quatre États. Il entrera en vigueur après avoir été ratifié par cinq États.

(2) Le nom exact de la directive « Police – Justice » est directive relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des

Les liens entre la convention 108 du Conseil de l'Europe et le droit de l'Union européenne sont étroits.

Ainsi, le considérant 105 du RGPD énonce que, lorsque la Commission européenne évalue la situation d'un pays tiers en vue de l'adoption d'une décision d'adéquation permettant le transfert de données à caractère personnel entre l'Union européenne et ce pays tiers, l'adhésion de ce pays tiers à la convention du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel et à son protocole additionnel doit être prise en compte.

La complémentarité entre le droit de l'Union européenne et la future convention 108 + est manifeste concernant le RGPD. Il s'agit de deux instruments permettant d'assurer un haut niveau de protection de la vie privée et des données à caractère personnel.

Si la convention du Conseil de l'Europe est moins détaillée que le RGPD et la directive « Police – Justice », elle repose sur des principes communs : le principe de finalité, le principe de proportionnalité et de pertinence, le principe d'une durée de conservation limitée, le principe de sécurité, l'existence de droits pour les personnes tels que les droits d'accès aux données, le droit de rectification ou encore le droit à l'effacement. De la même façon, les droits des personnes concernées, la protection de ces droits par les autorités de contrôle, ainsi que les obligations des responsables de traitement se trouvent réaffirmés.

Enfin, par une décision du 9 avril 2019, le Conseil de l'Union européenne a autorisé les États membres de l'Union à ratifier la convention 108 modernisée, dans l'intérêt de l'Union (1). Pour rappel, cette décision était nécessaire dans la mesure où le protocole couvre pour partie des domaines relevant de la compétence exclusive de l'Union européenne (2).

---

fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données

(1) https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32019D0682&from=EN

(2) *L'article 3, paragraphe 2, du TFUE prévoit que l'Union dispose d'une compétence exclusive pour la conclusion d'un accord international notamment lorsque cette conclusion est susceptible d'affecter des règles communes ou d'en altérer la portée. Or, dans le cas présent, le protocole n'était ouvert à la signature que des seuls États.*

Le Règlement général sur la protection des données,
outil juridique de référence pour la protection des données personnelles

Le règlement nº 2016/679, dit règlement général sur la protection des données (RGPD ou *General Data Protection Regulation*), est un règlement de l'Union européenne qui renforce et harmonise la protection des données personnelles au niveau européen. Définitivement adopté par le Parlement européen le 27 avril 2016 après quatre années de négociations entre États membres, il est entré en vigueur le 25 mai 2018 et demeure le texte de référence en matière de protection des données à caractère personnel, remplaçant la *directive sur la protection des données personnelles* adoptée en 1995. En France, il s'inscrit dans la continuité de la loi « Informatique et Libertés » du 6 janvier 1978 et renforce le contrôle par les citoyens de l'utilisation qui peut être faite des données les concernant.

Le RGPD s'applique à toute entité, indépendamment de sa taille, de son pays d'origine ou d'implantation, de son secteur d'activité ou la teneur des données récoltées. Toute organisation publique ou privée traitant des données pour son compte ou pour le compte d'un tiers est concernée dès lors qu'elle est établie et/ou que son activité cible des résidents européens.

Le RGPD impose aux organisations collectant des données personnelles un certain nombre de bonnes pratiques. Deux principes clés du RGPD encadrent la récolte des données : le principe de finalité, qui consacre la limitation des champs d'utilisation de la donnée, et le principe de minimisation, qui empêche la collecte des données non nécessaires à la réalisation des objectifs de l'entité concernée. Le RGPD affirme aussi le principe de transparence, qui oblige les organisations à communiquer sur la récolte de données et à informer de l'utilisation qui est faite de ces données.

L'une des dispositions les plus remarquées du RGPD porte sur le droit au consentement des utilisateurs. Le RGPD impose un consentement libre, spécifique, éclairé et univoque, dont les conditions sont définies aux articles 4 et 7. Il s'agit d'un principe qui était déjà affirmé en France par loi de 1978 et que le RGPD est venu renforcer. Enfin, le RGPD fixe une durée déterminée pour la conservation des données personnelles. Les données doivent être détruites, anonymisées ou archivées à partir d'une date butoir déterminée par l'organisme en question. Le règlement européen fixe aussi un principe de sécurisation des données, qui impose aux responsables des données collectées de prendre des mesures pour garantir leur sécurité et éviter leur divulgation à des tiers non autorisés.

L'application concrète du RGPD repose sur la mobilisation des régulateurs nationaux des États membres. Dans chaque pays, une autorité de la régulation numérique de référence est nommée. En France, c'est la Commission nationale de l'informatique et des libertés (CNIL) qui est chargée de vérifier et de faire respecter le RGPD aux organismes œuvrant sur le territoire français.

Sources diverses.

2. Un instrument auquel le droit national est déjà conforme

La proximité entre la convention 108 modernisée et les textes de droit européen explique également l'adaptation du droit national aux stipulations du texte du Conseil de l'Europe. En effet, le RGPD et la directive « Police-Justice » ont donné lieu à des mesures d'adaptation et de transposition dans le droit national, portées notamment par l'ordonnance n° 2018-1125 du 12 décembre 2018 prise en application de l'article 32 de la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles et portant modification de la loi n° 7817 du 6 janvier 1978, dite « informatique et libertés ».

Dès lors, comme le souligne l'étude d'impact du présent projet de loi, la convention 108 modernisée ne devrait pas nécessiter de mesures d'adaptation supplémentaires, tant dans les domaines couverts par la réglementation européenne que dans le domaine de la sécurité nationale et de la défense. Si l'**article 11** de cette convention permet aux États de prévoir des exceptions à plusieurs règles conventionnelles (1) pour des motifs tirés de la protection de la sécurité nationale et de la défense, les exceptions admises doivent être prévues par la loi et respecter l'essence des droits et libertés fondamentales tout en étant nécessaires et proportionnées dans une société démocratique. C'est le cas dans le droit national français, grâce à la loi informatique et libertés. En outre, la Partie française entend formuler une déclaration interprétative – dont le texte projeté est intégré à l'étude d'impact du présent projet de loi – afin de préciser l'étendue des exceptions en question.

Dans le cadre du comité de suivi de la convention 108, des travaux ont été engagés sur la portée des dérogations permises par l'**article 11** susmentionné. Ils visent à formaliser une note d'orientation qui permettrait notamment de clarifier, au bénéfice de tous les États Parties, les concepts-clés mentionnés dans l'**article 11** (sécurité nationale, défense, mesures nécessaires et proportionnées, etc.), et ce d'ici à la fin de l'année 2024.

(1) On peut citer les principes de loyauté, de transparence, de limitation des finalités, d'exactitude, de minimisation des données et de limitation de la conservation (article 5), l'obligation d'information des personnes concernées incombant au responsable de traitement (article 8) ou encore les pouvoirs et prérogatives des autorités de contrôle (article 15).

II. UN PROTOCOLE QUI VIENT RENFORCER LES GARANTIES APPORTÉES PAR LA CONVENTION 108 EN VUE DE PROTÉGER LES DONNÉES PERSONNELLES

Le protocole 223, qui compte à ce jour quarante-quatre États signataires et dix-sept États Parties l'ayant ratifié (1), entrera en vigueur le premier jour du mois suivant l'expiration d'une période de trois mois après la date à laquelle toutes les Parties à la convention 108 auront accepté, ratifié ou approuvé ledit protocole, conformément aux stipulations de son **article 37**. À défaut, il peut entrer en vigueur après la ratification de trente-huit Parties, mais seulement à l'expiration d'une période de cinq ans après la date d'ouverture à la signature, soit le 11 octobre 2023.

A. LE PROTOCOLE VISE À ADAPTER LE DROIT EXISTANT AUX ÉVOLUTIONS TECHNOLOGIQUES ET À L'INTENSIFICATION DES ÉCHANGES DE DONNÉES PERSONNELLES

Le protocole 223, qui comporte un préambule, quarante articles et une annexe, répond à la nécessité de moderniser les outils existants afin de répondre, d'une part, aux évolutions technologiques associées à l'utilisation de nouvelles technologies de l'information et de la communication et, d'autre part, à l'intensification des échanges de données personnelles à l'échelle internationale. Cet objectif de modernisation est étroitement lié au second objectif poursuivi par le protocole, à savoir le renforcement des garanties de mise en œuvre de la convention.

Afin de poursuivre ce double objectif, le protocole 223 prévoit notamment (voir tableau en annexe) :

- l'application des principes de protection des données à l'ensemble des traitements (**articles 1 à 3**) ;

- le renforcement des exigences relatives aux principes de proportionnalité et de minimisation des données, et de licéité du traitement, ainsi que de nouveaux droits accordés aux personnes dans le contexte de prises de décision basées sur des algorithmes (**article 5**) ;

- l'élargissement de la catégorie des données sensibles, qui comprend désormais les données génétiques et biométriques et celles relatives à l'appartenance à un syndicat et à l'origine ethnique (**article 6**) ;

- l'obligation de notifier les violations de données, ainsi qu'une plus grande transparence concernant les traitements de données (**article 7**) ;

---

(1) *https://www.coe.int/fr/web/conventions/full-list?module=signatures-by-treaty&treatynum=223*

- le renforcement de la responsabilité des responsables du traitement des données (**article 10**) ;

- la mise en place d'un régime clair des flux transfrontières de données (**article 14**) ;

- un renforcement des pouvoirs et de l'indépendance des autorités de protection des données, ainsi que des bases légales nécessaires à la coopération internationale (**articles 15 à 17**).

Le protocole va permettre la mise en œuvre de nouvelles procédures d'évaluation et d'examen de la convention, endossées par le comité consultatif associé à la convention en novembre 2021 et rendues publiques [(1)].

En cas de non-conformité, l'objectif du comité sera d'aider la Partie concernée ou le candidat à l'adhésion et ses autorités compétentes à se mettre en conformité au regard de la convention et de ses (futurs) engagements. Ces mesures recommandées devraient être de nature incitative et progressive :

- le comité peut donner des conseils et, si nécessaire, faciliter la mise en place d'une assistance de la part d'experts ;

- selon le cas, le comité peut inviter et/ou aider la Partie ou le candidat à l'adhésion concerné à élaborer un plan d'action pour l'amener à se mettre en conformité dans un délai qui sera convenu entre le comité et la Partie ou le candidat à l'adhésion concerné ;

- le comité peut inviter la Partie ou le candidat à l'adhésion concerné à soumettre des rapports sur les progrès réalisés pour se mettre en conformité au regard de ses engagements (futurs).

Dans le cas où aucune de ces mesures ne permettrait d'atteindre les résultats escomptés dans le délai imparti et si la Partie continue à ne pas respecter les engagements pris en vertu de la convention, d'autres mesures pourront être envisagées, notamment :

- l'organisation par le comité de visites à haut niveau ;

- le signalement de la non-conformité par le comité à l'organe du Conseil de l'Europe où siègent les États membres de l'organisation (Comité des Ministres) ;

- l'application éventuelle des dispositions prévues à l'article 60 de la convention de Vienne sur le droit des traités de 1969 (possibilité pour les autres Parties de suspendre l'application du traité à l'égard de l'État défaillant).

---

(1) *https://rm.coe.int/t-pd-2018-21rev11-fr-mechanisme-evaluation-examen-revised-clean/1680a497f0*

Il convient aussi de noter que l'**article 23** de la convention 108 modernisée transforme l'actuel comité consultatif en comité conventionnel. Dans le but de faciliter l'application pratique de la convention 108, pour ce qui est de son interprétation, un comité consultatif composé de représentants de toutes les Parties avait été prévu par la même convention pour formuler des propositions ou donner des avis à ces Parties en vue de trouver des solutions en réponse aux difficultés rencontrées.

Le comité conventionnel aura un rôle en partie identique au comité consultatif actuel en ce qu'il aura pour objectif commun de faciliter l'application et l'interprétation de la convention et, le cas échéant, de perfectionner celle-ci, notamment en ayant la capacité de proposer des amendements ~~à la convention~~ et d'examiner des propositions d'amendements formulées par une autre Partie ou par le Comité des Ministres.

Néanmoins, il aura aussi des pouvoirs plus étendus.

Tout d'abord, le comité conventionnel jouera un rôle clé dans l'évaluation du respect de la convention, soit par la préparation d'une évaluation du niveau de protection des données offertes par un candidat à l'adhésion (**article 23**, alinéa e) soit par l'examen périodique de l'application de la convention par les Parties (**article 23**, alinéa h), le but visé étant de garantir la mise en œuvre des principes de protection des données consacrés par le texte de la convention. À ce titre, le processus et les critères utilisés pour cette évaluation doivent être clairement définis dans le règlement du comité conventionnel : une procédure objective, équitable et transparente (et dont les modalités sont en cours de définition à l'occasion des travaux du comité de suivi) sera décrite en détail dans son règlement.

Le comité conventionnel aura également la faculté d'évaluer la conformité avec la convention du régime de protection des données d'un État ou d'une organisation internationale, à la demande des derniers (**article 23**, alinéa f). Il aura également la faculté d'approuver des modèles de garanties standardisées pour les transferts de données (**article 23**, alinéa g). Enfin, il pourra contribuer au règlement de toute difficulté surgissant entre les Parties (**article 23**, alinéa i). En cas de différends, le comité conventionnel s'efforcera de parvenir à un règlement par la négociation ou par tout autre moyen amiable.

B. LE RENFORCEMENT JURIDIQUE DE LA PROTECTION DES DONNÉES PERSONNELLES DOIT S'ACCOMPAGNER D'UN SOUTIEN ACCRU À LA MISE EN ŒUVRE DES RÈGLES DE DROIT

Pour la rapporteure, la consolidation des règles juridiques en matière de protection des données personnelles doit s'accompagner d'une vigilance accrue sur les capacités de mise en œuvre de ces règles par les acteurs concernés. C'est ce qu'illustre l'affaire de l'application Gendnotes, utilisée par la gendarmerie. Celle-ci croisait des données sensibles comme les orientations sexuelles ou politiques et

les partageaient avec d'autres services. De plus, la consolidation de ces règles juridiques amène à réévaluer les moyens financiers et humains employés à cette fin.

La mise en œuvre du RGPD et de façon générale l'adaptation des outils juridiques aux évolutions technologiques se sont traduites par de nouvelles missions pour les acteurs spécialisés tels que la CNIL, mais aussi pour les usagers, comme en atteste en France l'exemple de l'Éducation nationale. Dès lors, si la ratification par notre pays du protocole 223 ne devrait pas nécessiter d'adaptations juridiques internes (voir *supra*), elle invite à apporter une attention renouvelée à la mise en œuvre des règles de droit dans le domaine du numérique.

1. L'exemple d'un acteur spécialisé : la Commission nationale de l'informatique et des libertés

Au plan administratif, l'entrée en vigueur du protocole pourra avoir des conséquences concernant les mécanismes d'évaluation et de mise en œuvre de la convention modernisée. En effet, la CNIL, en tant qu'autorité de contrôle en charge de veiller au respect des stipulations de ce texte, sera sollicitée dans le cadre de la mise en œuvre du mécanisme au moment de l'entrée en vigueur de la convention 108+ pour évaluer la conformité de la France et au moment de la mise en œuvre de la procédure de suivi à l'égard de notre pays. La CNIL devra ainsi mobiliser des ressources au sein de ses différents services en vue d'apporter des contributions sur les questions spécifiques à l'exercice de ses pouvoirs, missions et actions en lien avec la mise en œuvre de la convention, et de manière plus générale, sur des questions transversales portant sur les règles substantielles de protection des données.

La CNIL est également concernée par le chapitre IV de la convention, qui traite de l'entraide entre les parties. En effet, la CNIL a été désignée pour assurer la mise en œuvre de ce pan du texte en France, qui se traduira par :

- une assistance mutuelle entre les autorités désignées en matière de contrôle ;

- des échanges d'informations (bilatéraux, multilatéraux ou par l'intermédiaire du Conseil de l'Europe) ;

- une assistance aux personnes concernées ayant leur résidence à l'étranger.

Enfin, la CNIL participe aux travaux du comité consultatif (futur comité conventionnel, évoqué précédemment), au sein de la délégation française menée par le ministère de l'Europe et des affaires étrangères.

Les missions afférentes à la convention 108 s'inscrivent dans une dynamique plus générale pour la CNIL, alimentée par plusieurs facteurs, parmi lesquels on peut citer :

- « l'européanisation » de la chaîne répressive dans le cadre du RGPD. Ainsi, pour un traitement transnational, les autorités de protection des données des États membres concernés sont compétentes pour s'assurer de la conformité des traitements de données mis en œuvre. Toutefois, le RGPD prévoit aussi un mécanisme de « guichet unique » dans le but d'assurer une réponse unique pour l'ensemble du territoire de l'Union européenne : les organismes ont pour interlocuteur l'autorité de protection des données du pays de leur établissement principal, dite autorité cheffe de file, qui doit coopérer avec les autorités de protection des données concernées. La CNIL est ainsi engagée à ce jour dans 97 procédures en tant qu'autorité cheffe de file et dans 400 en tant qu'autorité concernée ;

- le principe de responsabilisation des acteurs, également introduit par le RGPD, s'est accompagné de nombreuses demandes de conseils adressées à la CNIL, qui a créé un nouveau « service de l'accompagnement et des délégués à la protection des données ».

En outre, les nouvelles législations européennes (*Digital services act*, *Data governance act*, *Artificial intelligence act* [(1)], etc.) pourraient amener la CNIL à exercer de nouvelles missions en fonction des compétences qui lui seront attribuées sur tout ou partie de ces textes.

Si le budget de la CNIL a été augmenté pour tenir compte notamment des nouvelles missions liées à l'application du RGDP, passant de 17 678 025 euros en 2018 à 24 303 403 euros en 2022, les moyens humains restent insuffisants au regard de l'étendue des missions. Plusieurs enjeux susceptibles de ne pouvoir être suffisamment pris en compte faute de moyens ont été signalés par la Commission nationale informatique et libertés à la rapporteure : prévention de l'affaiblissement de la chaîne de contrôle et réduction de l'écart entre la capacité de contrôle de la CNIL et la taille et complexité de l'écosystème à contrôler, assurance de sécurité juridique pour les opérateurs lorsqu'ils consultent ou saisissent la Commission nationale informatique et libertés [(2)], instruction dans des délais restreints de volumes de plaintes très importants [(3)] et traitement des notifications de violations de données [(4)].

---

(1) Le DSA doit être formellement adopté par le Conseil de l'Union européenne le 4 octobre en vue d'une entrée en vigueur en 2024, le Data Governance Act a été adopté en mai 2022 et doit entrer en vigueur en septembre 2023, l'Artificial Intelligence Act a été présenté au premier semestre 2021.

(2) En 2021, 161 475 appels ont été reçus, 16 898 requêtes ont été reçues par voie électronique, le site web de la CNIL a été visité 10 809 884 fois et 576 dossiers ont été traités.

(3) 14 143 plaintes ont été reçues par la CNIL en 2021, soit 4 % de plus qu'en 2020.

(4) 5 037 violations de données ont été notifiées en 2021.

2. L’exemple de l’Éducation nationale : la nécessité de porter une attention particulière aux usagers du numérique

La charge induite par l’application des nouvelles réglementations en matière de numérique et de protection des données personnelles vaut aussi pour les acteurs non spécialisés, usagers des outils numériques, comme en atteste l’exemple de l’Éducation nationale.

D’une part, un effort a été fait pour développer la formation des enseignants au et par le numérique, autour de plusieurs dispositifs qui associent les académies et le réseau Canopé (1), à commencer par la plateforme de formation hybride des agents M@gistère. Cette plateforme propose des ressources de formation au numérique à l’attention de l’ensemble des agents du ministère de l’Éducation nationale et de la Jeunesse (MENJ). Par ailleurs, le MENJ s’est engagé dans une phase expérimentale de certification des compétences numériques incluant un volet sur les compétences d’enseignement à l’aide du numérique. Cette certification, qui s’appuie sur la plateforme PIX, comprend un volet dédié au respect du RGPD dans la pratique professionnelle. Il importe que cette démarche de certification soit soutenue avec des moyens suffisants par les académies, qui proposent désormais des formations et autres actions sur les territoires autour de la citoyenneté numérique, dans un esprit de promotion et de respect du RGPD. Il importe également de rappeler que « certifier n’est pas former », pour reprendre les termes du SNES-FSU, qui explique que PIX évalue entre autres ce que les élèves ont pu apprendre à titre personnel, en dehors du cadre scolaire, ce qui ne peut que renforcer les inégalités. Il apparaît donc essentiel de mettre l’accent sur la formation des élèves, qui passe d’abord par une formation et certification des enseignants eux-mêmes, mais aussi par un véritable investissement dans le matériel et les outils numériques.

Cet effort s’accompagne de la mise en place de nouveaux outils et équipements, qu’il s’agisse des « briques logicielles » développées par le MENJ pour filtrer le transfert des données personnelles des usagers (professeurs, élèves) aux éditeurs de ressources numériques ou des référentiels mis à la disposition des partenaires éditeurs, fabricants ou encore collectivités territoriales. En outre, le MENJ cherche à proposer aux usagers des alternatives aux GAFAM américains (Google, Amazon, Facebook, Apple, Microsoft) pour la visioconférence (Big Blue Button), la bureautique et l’hébergement de vidéo (Apps.education.fr), leur permettant d’avoir l’assurance d’une conformité RGPD.

Pour autant, les retours du terrain pour la mise en œuvre de la formation au et par le numérique en intégrant la réglementation du RGPD font ressortir la complexité et le manque d’interopérabilité entre les différents services (multi-authentifications, multi-saisies d’informations...). Au-delà de l’expérience de la crise liée à la pandémie de covid-19, qui avait contraint au printemps 2020 les enseignants à s’adapter dans des délais très restreints aux outils numériques sans

(1) Canopé est un opérateur public du MENJ ayant pour mission la formation au quotidien des enseignants

avoir nécessairement bénéficié de formation préalable et sans avoir nécessairement d'outils opérationnels à disposition, la bonne application des règles en matière de protection des données personnelles apparaît comme un enjeu à part entière dans la maîtrise des outils numériques. Le droit à la formation des personnels de l'Éducation Nationale se doit d'être renforcé, non pas seulement avec la plateforme M@gistère, qui a pour défauts de proposer essentiellement de l'auto-formation et d'être très méconnu du personnel de l'Éducation Nationale. Ce droit à la formation avec des formateurs de chair et d'os se heurte souvent à l'absence de remplaçants pour des absences de courte durée et au manque d'effectifs des AED (Assistants d'Éducation). Par ailleurs, ce sont les collectivités territoriales qui installent les logiciels sur les ordinateurs des établissements scolaires, et Google Chrome est ainsi largement utilisé comme navigateur. Nous pouvons nous interroger sur l'accompagnement des collectivités territoriales dans le domaine du numérique et du RGPD.

La rapporteure s'est notamment intéressée à la mise en œuvre des recommandations formulées dans un rapport élaboré par l'Inspection Générale de l'Éducation Nationale (IGEN) et l'Inspection Générale de l'Administration de l'Éducation Nationale et de la Recherche (IGAENR) en 2018 et portant sur les « données numériques à caractère personnel au sein de l'Éducation Nationale [(1)] ». En réponse à ces préconisations, de nouveaux dispositifs ont été mis en place pour l'information et la formation des personnels (voir *supra*) et un Comité d'éthique pour les données d'éducation a été lancé en 2019, afin d'apporter un encadrement à la production par l'Éducation Nationale d'un très grand nombre de données liées à la vie scolaire, aux évaluations et aux résultats des élèves, aux travaux et aux devoirs qu'ils réalisent. Le Comité d'éthique pour les données d'éducation, instance indépendante, a ainsi pour missions de conduire et développer la réflexion sur les aspects éthiques associés à l'utilisation des données d'éducation, afin de garantir un juste équilibre entre valorisation et protection de la donnée. Par ailleurs, des délégués à la protection des données ont été nommés au niveau national et des académies. Cependant, tout ceci demeure très opaque pour les personnels de l'Éducation Nationale, qui pour la plupart ignorent l'existence du Comité d'éthique pour les données d'éducation et des délégués à la protection des données.

Ceci étant posé, plusieurs projets sont actuellement en cours.

En application de l'article 40 du RGPD, un code de conduite est en cours d'élaboration par la filière professionnelle des Edtechs [(2)] et des éditeurs, pour une bonne application du RGPD dans le contexte particulier du Code de l'éducation. En effet, la conformité au RGPD d'une entreprise ne garantit pas sa conformité aux règles spécifiques de la collecte et du traitement des données dans un contexte scolaire. Le code de conduite implique l'adhésion des Edtechs et impose, solution

---

(1) https://www.education.gouv.fr/donnees-numeriques-caractere-personnel-au-sein-de-l-education-nationale-9434

(2) Soit l'ensemble des start-ups du numérique évoluant dans le secteur de l'éducation, de l'enseignement supérieur et de la formation professionnelle.

par solution, une certification de conformité délivrée par un organisme agréé. L'objectif fixé est une mise à disposition du code de conduite à compter de la rentrée 2023.

Par ailleurs, le MENJ a entamé une réflexion avec la CNIL sur la réalisation d'un référentiel des données scolaires sensibles au titre du RGPD, destiné à mieux accompagner l'encadrement de l'utilisation de ces données par la filière EdTech.

Enfin, un travail est en cours afin de diffuser une doctrine technique pour l'éducation qui a vocation à être rendue juridiquement opposable, afin d'apporter de nouvelles garanties sur l'utilisation des données scolaires.

Pour la rapporteure, cette dynamique doit être poursuivie et s'accompagner d'une attention particulière pour les usagers, et leur formation se doit donc d'être continue afin qu'ils puissent faire face aux évolutions juridiques et matérielles.

EXAMEN EN COMMISSION

Le mercredi 5 octobre 2022, la commission examine le projet de loi autorisant la ratification du Protocole d'amendement à la convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel.

M. le président Jean-Louis Bourlanges. Chers collègues, notre ordre du jour appelle ce matin l'examen de deux projets de loi dont nous sommes saisis en vue de la ratification d'un amendement à une convention et de l'approbation d'un accord international.

Le premier de ces textes est le projet de loi autorisant la ratification du protocole d'amendement à la convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel. Mme Ersilia Soudais est notre rapporteure pour ce texte.

En préambule, je rappellerai que la convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, dite « convention 108 », signée par la France le 28 janvier 1981, est l'un des très rares instruments juridiques contraignants en la matière. Cinquante-cinq États sont parties à ce traité : les quarante-six États membres du Conseil de l'Europe, ainsi que neuf États tiers (Argentine, Cap-Vert, Maroc, Maurice, Mexique, Russie, Sénégal, Tunisie et Uruguay).

Cette convention et son protocole additionnel nécessitaient d'être modernisés afin de répondre aux nouveaux défis que posent l'utilisation des nouvelles technologies de l'information et de la communication, ainsi que l'intensification et la mondialisation des échanges de données à l'ère du numérique, par rapport à la protection de la vie privée et des informations personnelles. Le protocole d'amendement signé par la France le 10 octobre 2018, dont le projet de loi en discussion vise à autoriser la ratification, a justement cette ambition, à telle enseigne que sa signature a conduit à requalifier la convention révisée en « convention 108 + ».

Pour faire bref, ce texte a un double objectif : renforcer le rôle des autorités de contrôle nationales – la Commission nationale de l'informatique et des libertés (CNIL), en France – et les garanties de mise en œuvre des protections prévues par la convention.

Mme Ersilia Soudais, rapporteure. Notre commission a été saisie du projet de loi autorisant la ratification du protocole d'amendement à la convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, dite « convention 108 ».

L'Assemblée nationale en débat après le Sénat, qui a adopté le projet de loi le 13 juillet 2021. Le protocole vise à moderniser une convention qui a été pionnière : elle est devenue, en 1981, le premier instrument juridique contraignant dans le domaine de la protection des données personnelles – et elle reste le seul à ce jour.

La convention, qui compte cinquante-cinq États parties, nécessite d'être modernisée, afin de répondre aux nouveaux défis que posent l'utilisation des nouvelles technologies de l'information et de la communication, ainsi que l'intensification des échanges de données personnelles à l'échelle internationale. Ces évolutions ont pu donner lieu à des coopérations mais elles ont aussi suscité des scandales, à la fois nationaux et internationaux : fuite de données ayant impliqué Facebook et la société Cambridge Analytica en 2016 ; recoupements de données de la caisse d'allocations familiales (CAF) pour détecter le profil de potentiels fraudeurs ; soupçons formulés par des organisations non gouvernementales (ONG) à propos de Doctissimo, qui aurait partagé des données confidentielles sur des plateformes, notamment américaines.

Une fois le protocole entré en vigueur, la nouvelle convention portera le nom de convention 108 +. À ce jour, le protocole, dit protocole 223, compte quarante-quatre États signataires, et dix-sept l'ont déjà ratifié.

Sans entrer dans le détail, ni de la convention, ni des modifications que le protocole va y apporter, je souhaite m'arrêter sur les enjeux qui me paraissent essentiels.

Tout d'abord, on peut saluer un effort de modernisation et de consolidation du droit. Le protocole s'inscrit lui-même dans une dynamique juridique. En effet, plusieurs outils ont été élaborés ces dernières années, notamment par l'Union européenne, pour fournir un cadre juridique au numérique. Comme vous le savez, le règlement général sur la protection des données (RGPD) a été adopté en 2016, de même que la directive dite police-justice. La convention 108 et son protocole additionnel reposent sur les mêmes principes que ces deux textes, à savoir : le principe de finalité ; le principe de proportionnalité et de pertinence ; le principe d'une durée de conservation limitée des données ; le respect des droits des personnes, notamment le droit d'accès aux données, le droit de rectification et le droit à l'effacement.

L'entrée en vigueur de la convention 108 + modernisée va donc consolider l'édifice juridique européen, avec une vocation extra-européenne qu'il faut souligner. En effet, la portée de la convention et du protocole dépasse le cadre régional du Conseil de l'Europe et de ses membres, puisque cinq États tiers ont déjà signé le protocole 223.

Parmi les principales modifications introduites par le protocole, on peut citer le renforcement des exigences relatives au principe de proportionnalité et de minimisation des données et à celui de licéité du traitement, ainsi que de nouveaux

droits accordés aux personnes dans le contexte de prises de décision basées sur des algorithmes, l'élargissement de la catégorie des données sensibles, qui comprend désormais les données génétiques et biométriques, ainsi que celles relatives à l'appartenance à un syndicat et à l'origine ethnique, ou encore un renforcement des pouvoirs et de l'indépendance des autorités de protection des données, ainsi que des bases légales nécessaires à la coopération internationale.

Le protocole introduit également de nouvelles procédures d'évaluation et d'examen de la convention, autour notamment d'un comité consultatif appelé à devenir comité conventionnel et dont les pouvoirs vont être étendus afin de favoriser la bonne application de la convention.

Je souhaite à présent attirer votre attention sur l'application de la convention, du point de vue des acteurs, spécialisés ou non dans le numérique, qui doivent veiller au quotidien au respect des règles protégeant les données personnelles. Cette question dépasse en pratique le seul champ de la convention 108 et du protocole 223 et concerne l'ensemble des textes partageant cet objectif, à commencer par le RGPD.

D'un côté, comme le souligne l'étude d'impact, l'entrée en vigueur de la convention 108 modernisée ne devrait pas nécessiter de mesures d'adaptation supplémentaires dans le droit national, dans la mesure où des modifications ont déjà été effectuées ces dernières années pour assurer sa conformité au RGPD et à la directive police-justice. Elles ont consisté en une modification de la loi du 6 janvier 1978 dite « informatique et libertés ». Ce sont également les dispositions de la loi informatique et libertés qui devront permettre à la France de prévoir quelques exceptions à l'application de la convention dans le domaine de la sécurité nationale et de la défense. Ces exceptions sont admises par la convention en son article 11, à la condition d'être prévues par la loi et de respecter l'essence des droits et libertés fondamentales tout en étant nécessaires et proportionnées dans une société démocratique.

D'un autre côté, la mise en œuvre de tous ces outils juridiques implique de nouvelles missions pour une série d'acteurs et une charge de travail parfois difficile à absorber. C'est notamment le cas des acteurs publics, qui ne disposent pas de moyens comparables à ceux des GAFAM et des autres géants du secteur. Je pense en particulier à la CNIL : puisqu'elle jouera le rôle d'autorité de contrôle au sens de la convention, elle sera sollicitée lorsque la France sera évaluée et elle participera toute l'année aux travaux du comité conventionnel. La CNIL est également concernée par le chapitre IV de la nouvelle convention, qui porte sur l'entraide entre les États parties. Elle a en effet été désignée pour mettre en œuvre ce pan de la convention du côté français, ce qui se traduira par des échanges accrus avec ses homologues.

Si le budget de la CNIL est passé de 17,7 millions d'euros en 2018 à 24,3 millions en 2022, pour tenir compte des nouvelles missions liées à l'application du RGPD, ses moyens humains restent insuffisants. Faute de

moyens, elle pourrait avoir des difficultés à remplir certaines de ses missions de contrôle ou à instruire dans des délais restreints des volumes de plaintes très importants.

Nous devons être d'autant plus vigilants que de nouvelles législations européennes vont entrer en vigueur dans le domaine du numérique dans les années à venir – le *Digital Services Act* (DSA), le *Data Governance Act* ou encore l'*Artificial Intelligence Act* –, qui seront de nature à créer de nouvelles missions pour la CNIL.

Ces inquiétudes ne valent pas que pour les acteurs spécialisés, mais aussi pour l'ensemble des usagers, qui sont également concernés par l'évolution et l'application des réglementations. J'ai choisi d'illustrer ce problème en évoquant un secteur que je connais bien : l'éducation nationale. Si des efforts ont été engagés en matière de formation des personnels au – et par – le numérique, il y a encore une marge de progression. La plateforme M@gistère, par exemple, a pour inconvénient de proposer essentiellement de l'auto-formation et d'être encore trop peu connue des enseignants.

De même, des postes de délégués à la protection des données ont été créés et un comité d'éthique pour les données d'éducation a été institué afin de développer la réflexion sur les aspects éthiques de l'utilisation des données d'éducation, mais cela reste opaque pour les personnels. On note les mêmes insuffisances, s'agissant de la formation des élèves. Elle est cruciale pour lutter contre les inégalités et la fracture numériques et elle revêt une importante dimension citoyenne. Néanmoins, la plateforme Pix met davantage l'accent sur la certification que sur la formation. La protection des données personnelles s'appuie sur des principes généraux mais elle doit aussi tenir compte des spécificités des différents secteurs. C'est en ce sens qu'une réflexion a été lancée pour élaborer un code de conduite visant à une bonne application du RGPD par la filière EdTech, qui réunit les *start-up* évoluant dans le numérique appliqué à l'éducation, l'enseignement supérieur et la formation professionnelle.

Les cas de la CNIL et de l'éducation nationale ne sont que deux exemples parmi d'autres. Ils montrent que la consolidation des règles juridiques en matière de protection des données personnelles doit s'accompagner d'une vigilance accrue quant aux capacités de mise en œuvre de ces règles par les acteurs concernés. Si nous n'y veillons pas, tout le dispositif risque d'être fragilisé et, avec lui, l'influence et la crédibilité de l'Europe dans un secteur qui reste dominé par les entreprises américaines et chinoises, dont la vigilance en matière de données personnelles est loin d'être toujours garantie.

Sous ces réserves, je vous invite à voter en faveur de la ratification de ce protocole.

M. le président Jean-Louis Bourlanges. Nous en venons aux questions des orateurs des groupes.

Mme Mireille Clapot (RE). L'Union européenne a été pionnière en matière de protection des données personnelles, avec le RGPD de 2016. La France, qui s'était déjà dotée, en 1978, d'une loi relative à l'informatique et aux libertés, l'a modifiée en 2018 pour prendre en compte le RGPD et la directive police-justice.

Dans le protocole qui nous est soumis, le périmètre géographique s'élargit au-delà de l'Union européenne, puisqu'il concerne le Conseil de l'Europe, et même des États tiers. La convention 108, ce sont cinquante-cinq États parties, et le protocole additionnel, quarante-quatre. Le protocole 223 adapte la loi au traitement, automatisé ou non, de données personnelles, précise le périmètre des données dites sensibles – données génétiques, biométriques, appartenance à un syndicat – et renforce les obligations des responsables de traitement de données et le pouvoir des autorités de contrôle.

Des audits relatifs aux applications accessibles *via* Facebook ont révélé que les 500 applications les plus téléchargées ont pu avoir accès aux photos, vidéos, descriptions, activités, événements, groupes, centres d'intérêt, likes, relations, statuts de 200 millions d'utilisateurs et de leurs amis ; de son côté, Yahoo aurait eu accès aux données d'au moins 123 millions d'utilisateurs sans aucune garantie quant à leur consentement. Ces données sont une mine d'or pour les annonceurs publicitaires. Rappelons-nous l'adage : « *Si c'est gratuit, c'est vous le produit* ». En l'occurrence, ce sont vos données.

Madame la rapporteure, vous avez évoqué le scandale qui a entouré Facebook et Cambridge Analytica : on a découvert à cette occasion que les données personnelles collectées à partir des réseaux sociaux de citoyens anglais, australiens et de 85 millions d'Américains avaient été utilisées pour mener des campagnes d'influence et de désinformation massive, qui ont eu un impact sur le cours de l'élection présidentielle américaine et la campagne du référendum sur le Brexit.

La donnée est à la fois un enjeu commercial et un outil de désinformation. Ce texte nous donne l'occasion de réaffirmer notre attachement aux valeurs européennes, par opposition à d'autres modèles. Nous voterons évidemment pour la ratification de ce protocole protecteur. Madame la rapporteure, pouvez-vous nous dire un mot du *Data Governance Act* et le *Data Act*, qui favorisent le partage des données et libèrent le potentiel de celles-ci ?

M. Frédéric Falcon (RN). La protection des données à caractère personnel est un enjeu majeur de sécurité et de souveraineté. Avec la numérisation de notre économie, l'essentiel des données numériques des Français est concentré dans les mains de quelques grandes entreprises présentes pour l'essentiel aux États-Unis, les GAFAM. Ces données personnelles sont à la disposition d'intérêts privés ; elles échappent à tout contrôle national, au risque d'être exploitées par des puissances étrangères à des fins économiques et géopolitiques.

Consciente de cette vulnérabilité, la Chine impose d'ores et déjà un contrôle strict des flux de données sortant de son territoire en bannissant toute entreprise, toute organisation ou tout réseau social susceptible de causer la fuite de données personnelles chinoises. Si le modèle chinois est excessif et constitue une menace pour les libertés, le rétablissement d'une souveraineté numérique à la française s'impose. Le Rassemblement national souhaite que les données des Français soient dorénavant hébergées par des entreprises françaises ou européennes, obligatoirement implantées en France ou dans l'Union. Le rachat des entreprises du numérique françaises par des groupes non-européens doit être limité, afin d'éviter tout transfert massif de données ou de technologies relatives à leur traitement

Le problème sous-jacent – et transversal – est l'extraterritorialité du droit américain. En effet, de nombreuses dispositions du droit américain peuvent être appliquées hors des frontières des États-Unis, à des personnes physiques ou morales, dans des pays tiers. Cela donne la possibilité aux juges américains d'engager des poursuites dans certains domaines, dont le droit de la concurrence et même la surveillance des données du monde entier, avec le *Clarifying Lawful Overseas Use of Data Act* (Cloud Act). Les entreprises européennes sont trop souvent sanctionnées par la justice américaine, qui leur ponctionne des milliards, au seul motif qu'elles effectuent, par exemple, des transactions en dollars avec des pays mis au ban. Il est urgent d'adopter des mesures protégeant nos intérêts : l'État américain a trop tendance à oublier qu'il existe un droit international.

De plus, soucieux de préserver les libertés des Français, nous souhaitons mettre fin à la censure qui sévit sur les réseaux sociaux. La modération est entre les mains d'algorithmes teintés d'idéologie, alors que cette attribution devrait revenir aux tribunaux français. De même, il n'est pas acceptable que certains citoyens se voient bannis des réseaux sociaux, ce qui est l'équivalent d'une mort sociale, au motif qu'ils ne partagent pas la ligne politique ou idéologique de quelques milliardaires désireux d'orienter l'opinion mondiale. Il est temps de créer un réseau social public, libre et gratuit.

La ratification du protocole d'amendement à la convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel reste une avancée timide ; elle est très insuffisante, au regard des enjeux auxquels nous sommes confrontés. Si nous déplorons ses carences, nous ne nous opposerons toutefois pas à sa ratification.

Mme Sabine Thillaye (DEM). Notre droit peine parfois à s'adapter aux évolutions technologiques, qui vont très vite et qui peuvent être la source de grands bouleversements, comme d'opportunités fabuleuses. L'utilisation des données a beaucoup évolué, sans qu'on prenne bien la mesure de ces changements.

Les données sont partout, constamment en train de se créer, de s'échanger, de s'analyser : elles sont devenues le nouvel or noir. L'Union européenne a su être

aux avant-postes pour faire émerger une politique ambitieuse en matière de protection des données et surtout de protection de nos concitoyens européens, qui peuvent désormais, grâce au RGPD, récupérer leurs datas quand ils le souhaitent, ou en limiter le traitement. Nous ne pouvons donc que nous réjouir qu'à l'échelle du Conseil de l'Europe, une garantie supplémentaire soit introduite pour assurer la protection des consommateurs européens, et même au-delà : la convention 108 a été signée par-delà notre continent, ce qui prouve que ses règles sont sécurisantes.

Le protocole 223 apportera les changements qui s'imposent pour nous adapter aux évolutions technologiques mais aussi à l'internationalisation de l'échange des données. En ce sens, la redéfinition des principes de protection, ainsi que la suppression de la référence au territoire de l'État comme espace de protection sont des avancées notables.

De même, le renforcement des obligations en matière de traitement des données, notamment une plus grande transparence, l'obligation de notifier les violations des données ou encore l'établissement d'un régime clair des flux transfrontaliers, viendront compléter efficacement la réglementation communautaire. Cette protection sera d'autant plus effective que ce protocole introduit une autorité de contrôle à même d'aider les États à appliquer ces règles vertueuses.

Enfin, ce texte nous amène malgré tout à questionner l'efficacité de la protection des données à l'occasion d'échanges transfrontaliers. Dans un arrêt de 2020, la Cour de justice de l'Union européenne a invalidé le *Privacy shield*, un accord qui permettait de transférer des données entre l'Union et les États-Unis, faute de protections suffisantes de nos datas, face à une politique américaine trop extensive. Notre commission doit se pencher sur ces enjeux essentiels pour notre souveraineté et celle de l'Europe. Quoi qu'il en soit, le groupe Démocrate soutiendra évidemment ce texte, qui constitue une avancée importante.

M. Alain David (SOC). La convention 108, que le protocole 223 tend à compléter, est le premier instrument juridique véritablement contraignant sur ce sujet délicat de la protection des données personnelles et de leur traitement automatisé et informatique. L'importance de cette question a été démontrée de façon spectaculaire par des affaires récentes, qui ont déjà été évoquées : l'élection de Donald Trump ou les soupçons pesant sur Doctolib, par exemple.

Il importe effectivement de prêter une attention accrue aux acteurs qui seront amenés à assurer la mise en œuvre des règles de droit encadrant le secteur du numérique, tout particulièrement les acteurs publics, qui ne bénéficient pas de moyens équivalents à ceux des grandes entreprises du secteur.

Avec mes collègues du groupe des députés socialistes et apparentés, nous notons que ce protocole est parfaitement compatible avec notre droit national et les autres règlements de l'Union européenne en la matière. Nous voterons ce texte de ratification, qui constitue un indéniable progrès.

Mme Stéphanie Kochert (HOR). Le protocole d'amendement qui nous est soumis est essentiel. Il va moderniser la convention 108 pour nous permettre de faire face à des évolutions technologiques majeures, à l'heure où nos concitoyens s'inquiètent de l'usage que les géants du numérique font de leurs données. Ce protocole marque clairement le lien qui existe entre la protection des données et l'ensemble des libertés fondamentales protégées par la convention européenne des droits de l'Homme. Ce lien est primordial : sans la protection des données, ce sont toutes les libertés publiques qui pourraient être menacées.

Ce protocole s'articulera sans difficulté avec notre droit interne. En effet, les nouvelles prérogatives qui sont accordées aux autorités de contrôle sont déjà, pour l'essentiel, celles qu'assume la CNIL en France. Au niveau européen, cette convention consacre des principes déjà établis dans le RGPD. Le fait que ces principes soient adoptés par les pays du Conseil de l'Europe et, plus largement, à l'international, montre une nouvelle fois la capacité du marché européen à exporter ses normes par consensus, au-delà de ses frontières. Enfin, à ceux qui s'inquiéteraient de voir cet outil de libéralisation des flux de données limiter la capacité des États à contrôler les données des personnes pour des raisons de sécurité et de défense, le protocole d'amendement prévoit de nombreuses garanties, qui paraissent suffisamment protectrices des libertés de chacun. Pour toutes ces raisons, le groupe Horizons et apparentés votera ce projet de loi de ratification.

Mme Estelle Youssouffa (LIOT). La convention pour la protection des personnes à l'égard du traitement automatisé et son protocole additionnel nécessitent d'être modernisés afin de répondre aux nouveaux défis que posent l'utilisation des nouvelles technologies, ainsi que l'intensification et la mondialisation des échanges de données personnelles. Il est impossible pour moi, en ce mois d'octobre rose, qui marque la lutte contre le cancer du sein, de ne pas poser la question du risque particulier que posent le stockage des données personnelles et leur pillage pour la protection du droit à l'oubli des survivants du cancer.

Cette convention est le premier et le seul instrument international juridique contraignant existant à ce jour. Le projet de loi de ratification intègre notamment les grands principes du RGPD et de la directive « police-justice ». Pour toutes ces raisons, le groupe Libertés, indépendants, outre-mer et territoires votera ce projet de loi, afin de garantir une plus grande protection des données personnelles de nos concitoyens.

Notre groupe espère que la ratification de ce texte permettra de diffuser le modèle européen en matière de protection des données mais également de renforcer notre culture du respect des données personnelles et de leur protection, qui présente encore des lacunes. Je pense notamment à la culture juridique de nos administrations et entreprises. L'une des recommandations de Mme la rapporteure est d'accorder plus de moyens, notamment humains, à la CNIL, pour qu'elle puisse remplir pleinement sa mission. Ce sera d'autant plus nécessaire que le

renforcement des autorités de contrôle nationales prévu par le protocole 223 lui attribuera de nouvelles missions.

M. Nicolas Dupont-Aignan (NI). La protection des données est un enjeu fondamental pour nos libertés, pour nos finances et pour notre souveraineté. Je n'ai pas de remarque particulière à faire sur la convention mais j'aimerais tout de même interroger la rapporteure sur cette phrase, qui figure à l'article 22, alinéa 4 : « *Toute partie qui n'est pas membre du Conseil de l'Europe contribuera au financement des activités du comité conventionnel* ». Il ne faudrait pas faire comme dans l'Organisation mondiale de la santé (OMS), où l'on intègre des parties, qui financent l'organisation et finissent par l'influencer. Pouvez-vous me rassurer sur ce point ?

Ce qui me frappe, c'est l'écart entre l'ambition affichée par les textes de loi, qui se multiplient, et la pratique. On a parlé de Doctolib et du danger qui pèse sur nos données de santé ; quand on voit la manière dont les autorités publiques françaises collaborent avec des entreprises américaines pour gérer nos systèmes informatiques, y compris ceux du ministère de la défense, il y a aussi de quoi s'inquiéter.

Madame la rapporteure, vous avez raison de poser la question des moyens de la CNIL. J'appelle aussi votre attention sur l'articulation entre la CNIL et l'Autorité de régulation de la communication audiovisuelle et numérique (ARCOM), et sur la nécessité de surveiller les GAFAM, qui peuvent exercer une véritable influence et aller jusqu'à censurer certaines personnalités.

Je me demande aussi ce qu'il reste de l'expertise nationale. Au fil du temps, on a de plus en plus délégué cette question à l'Union européenne, qui la gère au travers de grandes directives, et qui négocie ensuite avec les États-Unis. Vous êtes tous au courant du bras de fer qui oppose les GAFAM et la Commission européenne au sujet de l'application du RGPD et du contrôle de ces fameuses entreprises américaines. Une âpre négociation a eu lieu entre Joe Biden et Ursula von der Leyen et, pour l'instant, la Commission s'est couchée, même si la négociation continue.

Monsieur le président, notre commission ne pourrait-elle pas produire un rapport sur ce secteur où les GAFAM, par leur rapidité d'action et leur puissance, devancent très largement la réaction des États et même de la Commission européenne ? Il importe que notre nation ne délègue pas tout à l'Union européenne, qui est elle-même très dépendante des États-Unis. Il y va de notre souveraineté, de notre capacité financière et de la liberté de nos concitoyens.

Mme Ersilia Soudais, rapporteure. Le *Data Act* et le *Data Government Act* sont des règlements européens, qui ont été adoptés en 2022 mais qui entreront en vigueur en septembre 2023. Ils ne concernent que les pays membres de l'Union européenne, alors que la convention 108 a une vocation beaucoup plus large. Mais

cela ne veut pas dire que le *Data Act* et le *Data Government Act* n'ont pas vocation à faire des émules !

Monsieur Falcon, vous avez parlé des milliardaires qui censurent certains de nos concitoyens sur les réseaux sociaux. Il est vrai que cela devrait rester du ressort des tribunaux. Mais veillons aussi à ce que la presse elle-même reste protégée des milliardaires. Défendons notre service public de l'information.

Globalement, nous sommes tous d'accord pour dire que ce texte, qui va renforcer la protection des données, est une bonne chose. Mais je vous invite à être très vigilants lors de l'examen du PLF. La CNIL a clairement exprimé son inquiétude et il faut veiller à lui donner des moyens suffisants pour qu'elle puisse remplir toutes ses missions. Faire des traités, c'est bien, mais avoir les moyens de les appliquer, c'est mieux.

Une loi du 28 février 2022 consacre le droit à l'oubli dans le domaine de l'assurance emprunteur pour les personnes ayant souffert d'un cancer. Il y a encore des progrès à faire concernant les données, qui peuvent fuiter à l'international.

Je veux enfin rassurer M. Dupont-Aignan, qui s'est inquiété de possibles ingérences dans le comité conventionnel : chaque État reste maître, contrairement à ce qui se passe à l'OMS.

M. le président Jean-Louis Bourlanges. Je dois dire que je suis saisi d'un vertige quand je considère l'ampleur du problème posé. Saurons-nous trouver un équilibre entre la nécessaire protection des données et l'absence de contraintes bureaucratiques trop lourdes ? Il me semble, mais je ne suis pas connaisseur de ces questions, que nous sommes encore loin d'avoir trouvé une solution optimale.

Je vous félicite, madame la rapporteure, pour cet excellent travail. Votre rapport est de ceux que l'on conserve, bien après le vote de la loi.

Article unique (autorisation de la ratification du protocole d'amendement à la convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel)

La commission ***adopte*** *l'article unique* ***non modifié****.*

L'ensemble du projet de loi est ***ainsi adopté****.*

ANNEXE N° 1 : TEXTE ADOPTÉ PAR LA COMMISSION

Article unique

(Non modifié)

Est autorisée la ratification du Protocole d'amendement à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (ensemble une annexe), signé à Strasbourg le 10 octobre 2018, adopté par le Sénat le 13 juillet 2021, dont le texte est annexé à la présente loi.

N.B. : Le texte de la convention figure en annexe au projet de loi (n° 5)

ANNEXE N° 2 : TABLEAU COMPARATIF CONVENTION 108 / CONVENTION 108 +

TEXTE ACTUEL DE LA CONVENTION ET PROTOCOLE ADDITIONNEL	CONVENTION MODERNISÉE 108+
Préambule	**Préambule**
Les États membres du Conseil de l'Europe, signataires de la présente Convention,	Les États membres du Conseil de l'Europe, et les autres signataires de la présente Convention,
Considérant que le but du Conseil de l'Europe est de réaliser une union plus étroite entre ses membres, dans le respect notamment de la prééminence du droit ainsi que des droits de l'homme et des libertés fondamentales ;	Considérant que le but du Conseil de l'Europe est de réaliser une union plus étroite entre ses membres, dans le respect notamment de la prééminence du droit ainsi que des droits de l'homme et des libertés fondamentales ;
Considérant qu'il est souhaitable d'étendre la protection des droits et des libertés fondamentales de chacun, notamment le droit au respect de la vie privée, eu égard à l'intensification de la circulation à travers les frontières des données à caractère personnel faisant l'objet de traitements automatisés ;	Considérant qu'il est nécessaire de garantir la dignité humaine ainsi que la protection des droits de l'homme et des libertés fondamentales de toute personne, et, eu égard à la diversification, à l'intensification et à la mondialisation des traitements des données et des flux de données à caractère personnel, l'autonomie personnelle, fondée sur le droit de la personne de contrôler ses propres données à caractère personnel et le traitement qui en est fait ;
Réaffirmant en même temps leur engagement en faveur de la liberté d'information sans considération de frontières ;	Rappelant que le droit à la protection des données à caractère personnel est à considérer au regard de son rôle dans la société et qu'il est à concilier avec d'autres droits de l'homme et libertés fondamentales, dont la liberté d'expression ;
	Considérant que la présente Convention permet de prendre en compte, dans la mise en œuvre des règles qu'elle fixe, le principe du droit d'accès aux documents officiels ;

Reconnaissant la nécessité de concilier les valeurs fondamentales du respect de la vie privée et de la libre circulation de l'information entre les peuples,	Reconnaissant la nécessité de promouvoir les valeurs fondamentales du respect de la vie privée et de la protection des données à caractère personnel à l'échelle mondiale, favorisant ainsi la libre circulation de l'information entre les peuples ;
	Reconnaissant l'intérêt d'intensifier la coopération internationale entre les Parties à la Convention.
Sont convenus de ce qui suit :	Sont convenus de ce qui suit :
Chapitre I – Dispositions générales	**Chapitre I – Dispositions générales**
Article 1er – Objet et but	**Article 1er – Objet et but**
Le but de la présente Convention est degarantir, sur le territoire de chaque Partie, à toute personne physique, quelles que soient sa nationalité ou sa résidence, le respect de ses droits et de ses libertés fondamentales, et notamment de son droit à la vie privée, à l'égard du traitement automatisé des données à caractère personnel la concernant (« protection des données »).	Le but de la présente Convention est de protéger toute personne physique, quelle que soit sa nationalité ou sa résidence, à l'égard du traitement des données à caractère personnel, contribuant ainsi au respect de ses droits de l'homme et de ses libertés fondamentales et notamment du droit à la vie privée.
Article 2 – Définitions	**Article 2 – Définitions**
Aux fins de la présente Convention :	Aux fins de la présente Convention :
a) « données à caractère personnel » signifie : toute information concernant une personne physique identifiée ou identifiable (« personne concernée ») ;	a) « données à caractère personnel » signifie : toute information concernant une personne physique identifiée ou identifiable (« personne concernée ») ;
b) « fichier automatisé » signifie tout ensemble d'informations faisant l'objet d'un traitement automatisé ;	Supprimé
c) « traitement automatisé » s'entend des opérations suivantes effectuées en totalité ou en partie à l'aide de procédés automatisés : enregistrement des données, application à ces données d'opérations logiques et/ou arithmétiques, leur modification, effacement, extraction ou diffusion ;	b) « 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 ;

	c) Lorsqu'aucun procédé automatisé n'est utilisé, le traitement de données désigne une opération ou des opérations effectuée(s) sur des données à caractère personnel au sein d'un ensemble structuré de données qui sont accessibles ou peuvent être retrouvées selon des critères spécifiques ;
d) « maître du fichier » signifie : la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui est compétent selon la loi nationale, pour décider quelle sera la finalité du fichier automatisé, quelles catégories de données à caractère personnel doivent être enregistrées et quelles opérations leurseront appliquées.	d) « responsable du traitement » signifie : 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 » 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 ;
	f) « sous-traitant » signifie : la personne physique ou morale, l'autorité publique, le service, l'agence ou tout autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement.
Article 3 – Champ d'application	**Article 3 – Champ d'application**
1. Les Parties s'engagent à appliquer la présente Convention aux fichiers et aux traitements automatisés de données à caractère personnel dans les secteurs public et privé.	2. Chaque Partie s'engage à appliquer la présente Convention aux traitements de données relevant de sa juridiction dans les secteurs public et privé, garantissant ainsi à toute personne le droit à la protection de ses données à caractère personnel.
3. Tout État peut, lors de la signature oudu dépôt de son instrument de ratification, d'acceptation, d'approbation ou d'adhésion, ou à tout moment ultérieur, faire connaître par déclaration adressée au Secrétaire Général du Conseil de l'Europe :	2. La présente Convention ne s'applique pas au traitement de données effectué par une personne dans le cadre d'activités exclusivement personnelles ou domestiques.

a) qu'il n'appliquera pas la présenteConvention à certaines catégories de fichiers automatisés de données à caractère personnel dont une liste sera déposée. Il ne devra toutefois pas inclure dans cette liste des catégories de fichiers automatisés assujetties selon son droit interne à des dispositions de protection des données. En conséquence, il devra amender cette listepar une nouvelle déclaration lorsque des catégories supplémentaires de fichiers automatisés de données à caractère personnel seront assujetties à son régime de protection des données ;	Supprimé
b) qu'il appliquera la présente Convention également à des informations afférentes à des groupements, associations, fondations, sociétés, corporations ou à tout autre organisme regroupant directement ou indirectement des personnes physiques et jouissant ou non de la personnalité juridique ;	Supprimé
c) qu'il appliquera la présente Convention également aux fichiers de données à caractère personnel ne faisant pas l'objet de traitements automatisés.	Supprimé
3. Tout État qui a étendu le champ d'application de la présente Convention par l'une des déclarations visées aux alinéas 2.b ou c ci-dessus peut, dans ladite déclaration, indiquer que les extensions ne s'appliqueront qu'à certaines catégories de fichiers à caractère personnel dont la liste sera déposée.	Supprimé
4. Toute Partie qui a exclu certaines catégories de fichiers automatisés de données à caractère personnel par la déclaration prévue à l'alinéa 2.a ci-dessus ne peut pas prétendre à l'application de la présente Convention à de telles catégories par une Partie qui ne les a pas exclues.	Supprimé

5. De même, une Partie qui n'a pas procédé à l'une ou à l'autre des extensions prévues aux paragraphes 2.b et c du présent article ne peut se prévaloir de l'application de la présente Convention sur ces points à l'égard d'une Partie qui a procédé à de telles extensions.	Supprimé
6. Les déclarations prévues au paragraphe n° 2 du présent article prendront effet au moment de l'entrée en vigueur de la Convention à l'égard de l'État qui les a formulées, si cet État les a faites lors de la signature ou du dépôt de son instrument de ratification, d'acceptation, d'approbation ou d'adhésion, ou trois mois après leur réception par le Secrétaire Général du Conseil de l'Europe si elles ont été formulées à un moment ultérieur. Ces déclarations pourront être retirées en tout ou en partie par notification adressée au Secrétaire Général du Conseil de l'Europe. Le retrait prendra effet trois mois après la date de réception d'une telle notification.	Supprimé
Chapitre II – Principes de base pour la protection des données	**Chapitre II – Principes de base pour la protection des données à caractère personnel**
Article 4 – Engagements des Parties	**Article 4 – Engagements des Parties**
7. Chaque Partie prend, dans son droit interne, les mesures nécessaires pour donner effet aux principes de base pour la protection des données énoncés dans le présent chapitre.	8. Chaque Partie prend, dans sa loi, les mesures nécessaires pour donner effet aux dispositions de la présente Convention ainsi que pour en assurer l'application effective.
9. Ces mesures doivent être prises au plus tard au moment de l'entrée en vigueur de la présente Convention à son égard.	2. Ces mesures doivent être prises par chaque Partie et doivent être entrées en vigueur au moment de la ratification ou de l'adhésion à la présente Convention.
	3. Chaque Partie s'engage : a) à permettre au Comité conventionnel prévu au chapitre VI d'évaluer l'efficacité des mesures qu'elle aura prises dans sa loi pour donner effet aux dispositions de la présente Convention ; et b) à contribuer activement à ce processus d'évaluation.

Article 5 – Qualité des données	**Article 5 – Légitimité du traitement de données et qualité des données**
	1. Le traitement de données doit être proportionné à la finalité légitime poursuivie et refléter à chaque étape du traitement un juste équilibre entre tous les intérêts en présence, qu'ils soient publics ou privés, ainsi que les droits et les libertés en jeu.
	2. Chaque Partie prévoit que le traitement de données ne peut être effectué que sur la base du consentement libre, spécifique, éclairé et non-équivoque de la personne concernée ou en vertu d'autres fondements légitimes prévus par la loi.
3. Les données à caractère personnel faisant l'objet d'un traitement automatisé sont :	3. Les données à caractère personnel faisant l'objet d'un traitement sont traitées licitement.
a) obtenues et traitées loyalement et licitement ;	
b) enregistrées pour des finalités déterminées et légitimes et ne sont pas utilisées de manière incompatible avec ces finalités ;	4. Les données à caractère personnel faisant l'objet d'un traitement sont : a) traitées loyalement et de manière transparente ; b) collectées pour des finalités explicites, déterminées et légitimes et ne sont pas traitées de manière incompatible avec ces finalités ; le traitement ultérieur à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique, ou à des fins statistiques est compatible avec ces fins, à condition que des garanties complémentaires s'appliquent ;
c) adéquates, pertinentes et non excessives par rapport aux finalités pour lesquelles elles sont enregistrées ;	c) adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont traitées ;
d) exactes et si nécessaire mises à jour ;	d) exactes, et si nécessaire, mises à jour ;
e) conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire aux finalités pour lesquelles elles sont enregistrées.	e) conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire aux finalités pour lesquelles elles sont traitées.

Article 6 – Catégories particulières de données	**Article 6 – Catégories particulières de données**
Les données à caractère personnel révélant l'origine raciale, les opinions politiques, les convictions religieuses ou autres convictions, ainsi que les données à caractère personnel relatives à la santé ou à la vie sexuelle, ne peuvent être traitées automatiquement à moins que le droit interne ne prévoie des garanties appropriées. Il en est de même des données à caractère personnel concernant des condamnations pénales.	1. Le traitement : - de données génétiques ; - de données à caractère personnel concernant des infractions, des procédures et des condamnations pénales et des mesures de sûreté connexes ; - de données biométriques identifiant un individu de façon unique ; - de données à caractère personnel pour les informations qu'elles révèlent sur l'origine raciale ou ethnique, les opinions politiques, l'appartenance syndicale, les convictions religieuses ou autres convictions, la santé ou la vie sexuelle ; n'est autorisé qu'à la condition que des garanties appropriées, venant compléter celles de la présente Convention, soient prévues par la loi. 2. Ces garanties doivent être de nature à prévenir les risques que le traitement de données sensibles peut présenter pour les intérêts, droits et libertés fondamentales de la personne concernée, notamment un risque de discrimination.
Article 7 – Sécurité des données	**Article 7 – Sécurité des données**
Des mesures de sécurité appropriées sont prises pour la protection des données à caractère personnel enregistrées dans des fichiers automatisés contre la destruction accidentelle ou non autorisée, ou la perte accidentelle, ainsi que contre l'accès, la modification ou la diffusion non autorisés.	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.

	2. Chaque Partie prévoit que le responsable du traitement est tenu de notifier, sans délai excessif, à tout le moins à l'autorité de contrôle compétente au sens de l'article 15 de la présente Convention, les violations des données susceptibles de porter gravement atteinte aux droits et libertés fondamentales des personnes concernées.
	Article 8 – Transparence du traitement
	1. Chaque Partie prévoit que le responsable du traitement informe les personnes concernées : - de son identité et de sa résidence ou lieu d'établissement habituels ; - de la base légale et des finalités du traitement envisagé des catégories des données à caractèrepersonnel traitées ; - le cas échéant, des destinataires ou catégories de destinataires des données à caractère personnel ; et - des moyens d'exercer les droits énoncés à l'article 9 ; ainsi que de toute autre information complémentaire nécessaire pour garantir un traitement loyal et transparent des données à caractère personnel. 2. Le paragraphe 1 ne s'applique pas lorsque la personne concernée détient déjà l'information.
	3. Lorsque les données à caractère personnel ne sont pas collectées directement auprès des personnesconcernées, 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 lui est impossible ou implique des efforts disproportionnés.
Article 8 – Garanties complémentaires pour la personne concernée	**Article9 – Droits des personnes concernées**
1. Toute personne doit pouvoir :	1. Toute personne a le droit :

a) connaître l'existence d'un fichier automatisé de données à caractère personnel, ses finalités principales, ainsi que l'identité et la résidence habituelle ou le principal établissement du maître du fichier ;	a) de ne pas être soumise à une décision l'affectant de manière significative, qui serait prise uniquement sur le fondement d'un traitement automatisé de données, sans que son point de vue soit pris en compte ;
b) obtenir à des intervalles raisonnables et sans délais ou frais excessifs la confirmation de l'existence ou non dans le fichier automatisé, de données à caractère personnel la concernant ainsi que la communication de ces données sous une forme intelligible ;	b) d'obtenir, à sa demande, à intervalle raisonnable et sans délai ou frais excessifs, la confirmation d'un traitement de données la concernant, la communication sous une forme intelligible des données traitées, et toute information disponible sur leur origine, sur la durée de leur conservation ainsi que toute autre information que le responsable du traitement est tenu de fournir au titre de la transparence des traitements conformément à l'article 8, paragraphe 1 ;
c) obtenir, le cas échéant, la rectification de ces données ou leur effacement lorsqu'elles ont été traitées en violation des dispositions du droit interne donnant effet aux principes de base énoncés dans les articles 5 et 6 de la présente Convention ; d) disposer d'un recours s'il n'est pas donné suite à une demande de confirmation ou, le cas échéant, de communication, de rectification ou d'effacement, visée aux paragraphes b et c du présent article.	c) d'obtenir, à sa demande, connaissance du raisonnement qui sous-tend le traitement de données, lorsque les résultats de ce traitement lui sont appliqués ; d) de s'opposer à tout moment, pour des raisons tenant à sa situation, à ce que des données à caractère personnel la concernant fassent l'objet d'un traitement, à moins que le responsable du traitement ne démontre des motifs légitimes justifiant le traitement qui prévalent sur les intérêts, ou les droits et libertés fondamentales de la personne concernée ;
	e) d'obtenir, à sa demande, sans frais et sans délai excessifs, la rectification de ces données ou, le cas échéant, leur effacement lorsqu'elles sont ou ont été traitées en violation des dispositions de la présente Convention ;
	f) de disposer d'un recours conformément à l'article 12, lorsque ses droits prévus par la présente Convention ont été violés ;
	g) de bénéficier, quelle que soit sa nationalité ou sa résidence, de l'assistance d'une autorité de contrôle au sens de l'article 15 pour l'exercice de ses droits prévus par la présente Convention.

	2. Le paragraphe 1.a ne s'applique pas si la décision est autorisée par une loi à laquelle est soumis le responsable du traitement et qui prévoit également des mesures appropriées pour la sauvegarde des droits, des libertés et des intérêts légitimes de la personne concernée.
	Article 10 – Obligations complémentaires
	1. Chaque Partie prévoit que les responsables du traitement, ainsi que, le cas échéant, les sous-traitants, doivent prendre toutes les mesures appropriées afin de se conformer aux obligations de la présente Convention et être en mesure de démontrer sous réserve de la législation nationale adoptée conformément à l'article 11, paragraphe 3, en particulier à l'autorité de contrôle compétente, prévue à l'article 15, que le traitement dont ils sont responsables est en conformité avec les dispositions de la présente Convention.
	2. Chaque Partie prévoit que les responsables du traitement, ainsi que, le cas échéant, les sous-traitants, doivent procéder, préalablement au commencement de tout traitement, à l'examen de l'impact potentiel du traitement de données envisagé sur les droits et libertés fondamentales des personnes concernées, et qu'ils doivent concevoir le traitement de données de manière à prévenir ou à minimiser les risques d'atteinte à ces droits et libertés fondamentales.
	3. Chaque Partie prévoit que les responsables du traitement, ainsi que, le cas échéant, les sous-traitants, prennent des mesures techniques et organisationnelles tenant compte des implications du droit à la protection des données à caractère personnel à tous les stades du traitement des données.

	4. Chaque Partie peut, eu égard aux risques encourus pour les intérêts, droits et libertés fondamentales des personnes concernées, adapter l'application des dispositions des paragraphes 1, 2 et 3 dans la loi donnant effet aux dispositions de la présente Convention, en fonction de la nature et du volume des données, de la nature, de la portée et de la finalité du traitement et, le cas échéant de la taille des responsables du traitement et des sous-traitants.
Article 9 – Exceptions et restrictions	**Article 11 – Exceptions et restrictions**
1. Aucune exception aux dispositions des articles 5, 6 et 8 de la présente Convention n'est admise, sauf dans les limites définies au présent article.	1. Aucune exception aux dispositions énoncées au présent chapitre n'est admise, sauf au regard des dispositions de l'article 5 paragraphe 4, de l'article 7 paragraphe 2, de l'article 8 paragraphe 1 et de l'article 9, dès lors qu'une telle exception est prévue par une loi, qu'elle respecte l'essence des droits et libertés fondamentales, et qu'elle constitue une mesure nécessaire et proportionnée dans une société démocratique :
2. Il est possible de déroger aux dispositions des articles 5, 6 et 8 de la présente Convention lorsqu'une telle dérogation, prévue par la loi de la Partie, constitue une mesure nécessaire dans une société démocratique :	Supprimé
a) à la protection de la sécurité de l'État, à la sûreté publique, aux intérêts monétaires de l'État ou à la répression des infractions pénales ;	2. à la protection de la sécurité nationale, à la défense, à la sûreté publique, à des intérêts économiques et financiers importants de l'État, à l'impartialité et à l'indépendance de la justice ou à la prévention, à l'investigation et à la répression des infractions pénales et à l'exécution des sanctions pénales, ainsi qu'à d'autres objectifs essentiels d'intérêt public général ;
b) à la protection de la personne concernée et des droits et libertés d'autrui.	b) à la protection de la personne concernée ou des droits et libertés fondamentales d'autrui, notamment la liberté d'expression.

3. Des restrictions à l'exercice des droits visés aux paragraphes b, c et d de l'article 8 peuvent être prévues par la loi pour les fichiers automatisés de données à caractère personnel utilisés à des fins de statistiques ou de recherches scientifiques, lorsqu'il n'existe manifestement pas de risques d'atteinte à la vie privée des personnes concernées.	4. Des restrictions à l'exercice des dispositions visées aux articles 8 et 9 peuvent être prévues par la loi pour le traitement des données utilisées à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques, lorsqu'il n'existe pas de risque identifiable d'atteinte aux droits et libertés fondamentales des personnes concernées.
	5. Outre les exceptions prévues au paragraphe 1 du présent article, relatives aux activités de traitement à des fins de sécurité nationale et de défense, chaque Partie peut prévoir par une loi et uniquement dans la mesure où cela constitue une mesure nécessaire et proportionnée dans une société démocratique à cette fin, des exceptions à l'article 4 paragraphe 3, à l'article 14 paragraphes 5 et 6 et à l'article 15 paragraphe 2, alinéas a, b, c et d. Cela est sans préjudice de l'exigence que les activités de traitement à des fins de sécurité nationale et de défense fassent l'objet d'un contrôle et d'une supervision indépendants effectifs selon la législation nationale de chaque Partie.
Article 10 – Sanctions et recours	**Article 12 – Sanctions et recours**
Chaque Partie s'engage à établir des sanctions et recours appropriés visant les violations aux dispositions du droit interne donnant effet aux principes de base pour la protection des données énoncés dans le présent chapitre.	Chaque Partie s'engage à établir des sanctions et des recours juridictionnels et non-juridictionnels appropriés visant les violations des dispositions de la présente Convention.
Article 11 – Protection plus étendue	**Article 13 – Protection plus étendue**
Aucune des dispositions du présent chapitre ne sera interprétée comme limitant ou portant atteinte à la faculté pour chaque Partie d'accorder aux personnes concernées une protection plus étendue que celle prévue par la présente Convention.	Aucune des dispositions du présent chapitre ne sera interprétée comme limitant ou portant atteinte à la faculté pour chaque Partie d'accorder aux personnes concernées une protection plus étendue que celle prévue par la présente Convention.

Chapitre III – Flux transfrontières de données	**Chapitre III – Flux transfrontières de données à caractère personnel**
Article12 – Flux transfrontières dedonnées à caractère personnel et droit interne	**Article14 – Flux transfrontières de données à caractère personnel**
1. Les dispositions suivantes s'appliquent aux transferts à travers les frontières nationales, quel que soit le support utilisé,de données à caractère personnel faisant l'objet d'un traitement automatisé ou rassemblées dans le but de les soumettre à un tel traitement.	Supprimé
2. Une Partie ne peut pas, aux seules finsde la protection de la vie privée, interdire ou soumettre à une autorisation spéciale les flux transfrontières de données à caractère personnel à destination du territoire d'uneautre Partie.	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.
3. Toutefois, toute Partie a la faculté de déroger aux dispositions du paragraphe 2 :	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 3. Un niveau de protection des données approprié peut être garanti par : a) a les règles de droit de cet État ou de cette organisation internationale, y compris les traités ou accords internationaux applicables ; ou

	b) des garanties ad hoc ou standardisées agréées, établies par des instruments juridiquement contraignants et opposables, adoptés et mis en œuvre par les personnes impliquées dans le transfert et le traitement ultérieur des données.
a) dans la mesure où sa législation prévoit une réglementation spécifique pour certaines catégories de données à caractère personnel ou de fichiers automatisés de données à caractère personnel, en raison de la nature de ces données ou de ces fichiers, sauf si la réglementation de l'autre Partie apporte une protection équivalente ;	4. Nonobstant les modalités prévues aux paragraphes précédents, chaque Partie peut prévoir que le transfert de données à caractère personnel peut avoir lieu : a) si la personne concernée a donné son consentement explicite, spécifique et libre, après avoir été informée des risques introduits par l'absence de garanties appropriées ; ou b) si des intérêts spécifiques de la personne concernée le nécessitent dans un cas particulier ; ou c) si des intérêts légitimes prépondérants, notamment des intérêts publics importants, sont prévus par la loi et si ce transfert constitue une mesure nécessaire et proportionnée dans une société démocratique ; ou d) si ce transfert constitue une mesure nécessaire et proportionnée dans une société démocratique pour la liberté d'expression.
	5. Chaque Partie prévoit que l'autorité de contrôle compétente au sens de l'article 15 de la présente Convention obtient toute information pertinente relative aux transferts de données prévus au paragraphe 3.b, et, sur demande, aux paragraphes 4.b et 4.c. 6. Chaque Partie prévoit également que l'autorité de contrôle peut exiger de la personne qui transfère les données qu'elle démontre l'effectivité des garanties prises ou l'existence d'intérêts légitimes prépondérants et qu'elle peut, pour protéger les droits et les libertés fondamentales des personnes concernées, interdire ou suspendre les transferts ou soumettre à

	condition de tels transferts de données.
b) lorsque le transfert est effectué à partir de son territoire vers le territoire d'un État non contractant par l'intermédiaire du territoire d'une autre Partie, afin d'éviter que de tels transferts n'aboutissent à contourner la législation de la Partie visée au début du présent paragraphe.	Supprimé
Article 2 – Flux transfrontières de données à caractère personnel vers un destinataire n'étant pas soumis à la juridiction d'une Partie à la Convention (Protocole additionnel)	Supprimé
1. Chaque Partie prévoit que le transfert de données à caractère personnel vers un destinataire soumis à la juridiction d'un État ou d'une organisation qui n'est pas Partie à la Convention ne peut être effectué que si cet État ou cette organisation assure un niveau de protection adéquat pour le transfert considéré.	Supprimé
2. Par dérogation au paragraphe 1 de l'article 2 du présent Protocole, chaque Partie peut autoriser un transfert de données à caractère personnel :	Supprimé
a) si le droit interne le prévoit :	Supprimé
– pour des intérêts spécifiques de la personne concernée, ou	Supprimé
– lorsque des intérêts légitimes prévalent, en particulier des intérêts publics importants, ou	Supprimé
b) si des garanties pouvant notamment résulter de clauses contractuelles sont fournies par la personne responsable du transfert, et sont jugées suffisantes par les autorités compétentes, conformément au droit interne.	Supprimé

Protocole additionnel	**Chapitre IV – Autorités de contrôle**
Article 1	**Article 15 – Autorités de contrôle**
1. Chaque Partie prévoit qu'une ou plusieurs autorités sont chargées de veiller au respect des mesures donnant effet, dans son droit interne, aux principes énoncés dans les chapitres II et III de la Convention et dans le présent Protocole.	1. Chaque Partie prévoit qu'une ou plusieurs autorités sont chargées de veiller au respect des dispositions de la présente Convention.
2. À cet effet, ces autorités : a) disposent notamment de pouvoirs d'investigation et d'intervention, ainsi que de celui d'ester en justice ou de porter à la connaissance de l'autorité judiciaire compétente des violationsaux dispositions du droit interne donnant effet aux principes visés au paragraphe 1 del'article 1 du présent Protocole.	2. À cet effet, ces autorités : a) disposent de pouvoirs d'investigation et d'intervention ; b) exercent les fonctions en matière de transferts de données prévues à l'article 14, notamment l'agrément de garanties standardisées ; c) c disposent du pouvoir de rendre des décisions relatives aux violations des dispositions de la présente Convention et peuvent, notamment, infliger des sanctions administratives ; d) disposent du pouvoir d'ester en justice ou de porter à la connaissance de l'autorité judiciaire compétente des violations des dispositions de la présente Convention ; e) sont chargées : de sensibiliser le public à leurs fonctions et à leurs pouvoirs, ainsi qu'à leurs activités ; f) de sensibiliser le public aux droits des personnes concernées et à l'exercice de ces droits ; g) de sensibiliser les responsables du traitement et les sous-traitants aux responsabilités qui leur incombent en vertu de la présente Convention ;

	h) une attention particulière sera portée au droit à la protection des données des enfants et des autres personnesvulnérables.
	3. Les autorités de contrôle compétentes sont consultées sur toute proposition législative ou administrative impliquant des traitements de données à caractère personnel
b) Chaque autorité de contrôle peut être saisie par toute personne d'une demande relative à la protection de ses droits et libertés fondamentales à l'égard des traitements de données à caractère personnel relevant de sa compétence.	4 Chaque autorité de contrôle compétente traite les demandes et les plaintes dont elle est saisie par les personnes concernées au regard de leurs droits à la protection des données et tient ces personnes informées des résultats.
3 Les autorités de contrôle exercent leurs fonctions en toute indépendance.	5. Les autorités de contrôle agissent avec indépendance et impartialité dans l'accomplissement de leurs fonctions et l'exercice de leurs pouvoirs et, ce faisant, elles ne sollicitent ni n'acceptent d'instructions.
	6. Chaque Partie s'assure que les autorités de contrôle disposent des ressources nécessaires à l'accomplissement effectif de leurs fonctions et à l'exercice de leurs pouvoirs. 7. Chaque autorité de contrôle prépare et publie un rapport d'activités périodique. 8. Les membres et agents des autorités de contrôle sont tenus à une obligation de confidentialité à l'égard des informations confidentielles auxquelles ils ont, ou ont eu, accès dans l'accomplissement de leurs fonctions et l'exercice de leurs pouvoirs.
4. Les décisions des autorités de contrôle faisant grief peuvent faire l'objet d'un recours juridictionnel.	9. Les décisions des autorités de contrôle peuvent faire l'objet d'un recours juridictionnel.
	10. Les autorités de contrôle ne sont pas compétentes s'agissant des traitements effectués par des organes dans l'exercice de leurs fonctions juridictionnelles.

5. Conformément aux dispositions du chapitre IV et sans préjudice des dispositions de l'article 13 de la Convention, les autorités de contrôle coopèrent entre elles dans la mesure nécessaire à l'accomplissement de leurs missions, notamment en échangeant toute informationutile.	Supprimé
Chapitre IV – Entraide	**Chapitre V – Coopération et entraide**
Article 13 – Coopération entre les Parties	**Article 16 – Désignation des autorités de contrôle**
1. Les Parties s'engagent à s'accorder mutuellement assistance pour la mise en œuvre de la présente Convention.	1. Les Parties s'engagent à coopérer et à s'accorder mutuellement assistance pour la mise en œuvre de la présente Convention.
2. À cette fin,	2. À cette fin,
a) chaque Partie désigne une ou plusieurs autorités dont elle communique la dénomination et l'adresse au Secrétaire Général du Conseil de l'Europe ;	a) chaque Partie désigne une ou plusieurs autorités de contrôle au sens de l'article 15 de la présente Convention, dont elle communique la dénomination et l'adresse au Secrétaire Général du Conseil de l'Europe ;
b) chaque Partie qui a désigné plusieurs autorités indique dans la communication visée à l'alinéa précédent la compétence de chacune de ces autorités.	b) chaque Partie, qui a désigné plusieurs autorités de contrôle, indique, dans la communication visée à l'alinéa précédent, la compétence de chacune.
3. Une autorité désignée par une partie la demande d'une autorité désignée par une autre Partie :	Supprimé
a) fournira des informations sur sondroit et sur sa pratique administrative en matière de protection des données ;	Supprimé
b) prendra, conformément à son droit interne et aux seules fins de la protection de la vie privée, toutes mesures appropriées pour fournir des informations de fait concernant un traitement automatisé déterminé effectué sur son territoire à l'exception toutefois des données à caractère personnel faisant l'objet de ce traitement.	Supprimé

	Article 17 – Formes de coopération
	4. Les autorités de contrôle coopèrent entre elles dans la mesure nécessaire à l'accomplissement de leurs fonctions et l'exercice de leurs pouvoirs, notamment : c) en s'accordant mutuellement une assistance par l'échange d'informations pertinentes et utiles et en coopérant entre elles, à condition qu'en ce qui concerne la protection des données à caractère personnel toutes les règles et garanties de la présente Convention soient respectées ; d) en coordonnant leurs investigations ou interventions, ou en menant des actions conjointes ; e) en fournissant des informations et des documents sur leur droit et sur leurs pratiques administratives en matière de protection des données.
	5. Les informations visées au paragraphe 1 n'incluent pas les données à caractère personnel faisant l'objet d'un traitement, à moins que ces données soient essentielles à la coopération ou que la personne concernée ait donné un consentement explicite, spécifique, libre et éclairé pour ce faire.
	6. Afin d'organiser leur coopération et d'accomplir les fonctions prévues aux paragraphes précédents, les autorités de contrôle des Parties se constituent en réseau.
Article 14 – Assistance aux personnes concernées ayant leur résidence à l'étranger	**Article 18 – Assistance aux personnes concernées**
1. Chaque Partie prête assistance à toute personne ayant sa résidence à l'étranger pour l'exercice des droits prévus par son droit interne donnant effet aux principes énoncés à l'article 8 de la présente Convention.	1. Chaque Partie prête assistance à toute personne concernée, quelle que soit sa nationalité ou sa résidence, pour l'exercice de ses droits prévus par l'article 9 de la présente Convention.

2. Si une telle personne réside sur le territoire d'une autre Partie, elle doit avoir la faculté de présenter sa demande par l'intermédiaire de l'autorité désignée par cette Partie.	2. Lorsque la personne concernée réside sur le territoire d'une autre Partie, elle doit avoir la faculté de présenter la demande par l'intermédiaire de l'autorité de contrôle désignée par cette Partie.
3. La demande d'assistance doit contenir toutes les indications nécessaires concernant notamment :	3. La demande d'assistance doit contenir toutes les indications nécessaires concernant notamment :
a) le nom, l'adresse et tous autres éléments pertinents d'identification concernant le requérant ;	a) a le nom, l'adresse et tout autre élément pertinent d'identification de la personne concernée à l'origine de la demande ;
b) le fichier automatisé de données à caractère personnel auquel la demande se réfère ou le maître de ce fichier ;	b) le traitement auquel la demande se réfère ou le responsable du traitement correspondant ;
c) le but de la demande.	c) l'objet de la demande.
Article 15 – Garanties concernant l'assistance fournie par les autorités désignées	**Article 19 – Garanties**
1. Une autorité désignée par une Partie qui a reçu des informations d'une autorité désignée par une autre Partie, soit à l'appui d'une demande d'assistance, soit en réponse à une demande d'assistance qu'elle a formulée elle-même, ne pourra faire usage de ces informations à des fins autres que celles spécifiées dans la demande d'assistance.	1. Une autorité de contrôle qui a reçu des informations d'une autre autorité de contrôle, soit à l'appui d'une demande, soit en réponse à une demande qu'elle a formulée elle-même, ne pourra faire usage de ces informations à des fins autres que celles spécifiées dans la demande.
2. Chaque Partie veillera à ce que les personnes appartenant ou agissant au nom de l'autorité désignée soient liées par des obligations appropriées de secret ou de confidentialité à l'égard de ces informations.	Supprimé
3. En aucun cas, une autorité désignée ne sera autorisée à faire, aux termes de l'article 14, paragraphe 2, une demande d'assistance au nom d'une personne concernée résidant à l'étranger, de sa propre initiative et sans le consentement exprès de cette personne.	2. En aucun cas une autorité de contrôle ne sera autorisée à faire une demande au nom d'une personne concernée, de sa propre initiative et sans l'approbation expresse de cette personne.

Article16 – Refus des demandes d'assistance	**Article 20 – Refus des demandes**
Une autorité désignée, saisie d'une demande d'assistance aux termes des articles 13 ou 14 de la présente Convention, ne peut refuser d'y donner suite que si :	Une autorité de contrôle, saisie d'une demande aux termes de l'article 17 de la présente Convention, ne peut refuser d'y donner suite que si :
a) la demande est incompatible avec les compétences, dans le domaine de la protection des données, des autorités habilitées à répondre ;	a) la demande est incompatible avec ses compétences ;
b) la demande n'est pas conforme aux dispositions de la présente Convention ;	b) la demande n'est pas conforme aux dispositions de la présente Convention ;
c) l'exécution de la demande serait incompatible avec la souveraineté, la sécurité ou l'ordre public de la Partie qui l'a désignée, ou avec les droits et libertés fondamentales des personnes relevant de lajuridiction de cette Partie.	c) l'exécution de la demande serait incompatible avec la souveraineté, la sécurité nationale ou l'ordre public de la Partie qui l'a désignée, ou avec les droits et libertés fondamentales des personnes relevant de la juridiction de cette Partie.
Article 17 – Frais et procédures de l'assistance	**Article 21 – Frais et procédures**
1. L'entraide que les Partiess'accordent aux termes de l'article 13, ainsi que l'assistance qu'elles prêtent aux personnes concernées résidant à l'étranger aux termes de l'article 14, ne donnera pas lieu au paiement des frais et droits autres que ceux afférents aux experts et aux interprètes. Ces frais et droits seront à la charge de la Partie qui a désigné l'autorité qui a fait la demande d'assistance.	1. La coopération et l'entraide que les Parties s'accordent aux termes de l'article 17, ainsi que l'assistance qu'elles prêtent aux personnes concernées aux termes des articles 9 et 18 ne donneront pas lieu au paiement de frais et droits autres que ceux afférents aux experts et aux interprètes. Ces frais et droits seront à la charge de la Partie qui a fait la demande.
2. La personne concernée ne peut êtretenue de payer, en liaison avec les démarches entreprises pour son compte sur le territoire d'une autre Partie, des frais et droits autres que ceux exigibles des personnes résidant sur le territoire de cette Partie.	2. La personne concernée ne peut être tenue de payer, en liaison avec les démarches entreprises pour son compte surle territoire d'une autre Partie, des frais et droits autres que ceux exigibles des personnes résidant sur le territoire de cette Partie.
3. Les autres modalités relatives à l'assistance concernant notamment les formes et procédures ainsi que les langues à utiliser seront établies directement entre les Parties concernées.	3. Les autres modalités relatives à la coopération et à l'entraide concernant notamment les formes et procédures ainsi que les langues à utiliser seront établies directement entre les Parties concernées.

Chapitre V – Comité consultatif	**Chapitre VI – Comité conventionnel**
Article 18 – Composition du comité	**Article 22 – Composition du comité**
1. Un comité consultatif est constitué après l'entrée en vigueur de la présente Convention.	1. Un Comité conventionnel est constitué après l'entrée en vigueur de la présente Convention.
2. Toute Partie désigne un représentant et un suppléant à ce comité. Tout État membre du Conseil de l'Europequi n'est pas Partie à la Convention a le droit de se faire représenter au comité par unobservateur.	2. Toute Partie désigne un représentant et un suppléant à ce Comité. Tout État membre du Conseil de l'Europe qui n'est pas Partie à la Convention a le droit de se faire représenter au comité par un observateur.
3. Le comité consultatif peut, par une décision prise à l'unanimité, inviter tout État non-membre du Conseil de l'Europe qui n'est pas Partie à la Convention à se faire représenter par un observateur à l'une de ses réunions.	3. Le Comité conventionnel peut, par une décision prise à la majorité des deux-tiers des représentants des Parties, inviter un observateur à se faire représenter à ses réunions.
	4. Toute Partie qui n'est pas membre du Conseil de l'Europe contribuera au financement des activités du Comité conventionnel selon des modalités établies par le Comité des Ministres en accord avec cette Partie.
Article 19 – Fonctions du comité	**Article 23 – Fonctions du comité**
Le comité consultatif :	Le Comité conventionnel :
a) peut faire des propositions en vue de faciliter ou d'améliorer l'application de la Convention ;	a) peut faire des recommandations en vue de faciliter ou d'améliorer l'application de la Convention ;
b) peut faire des propositions d'amendement à la présente Convention conformément à l'article 21 ;	b) peut faire des propositions d'amendement à la présente Convention conformément à l'article 25 ;
c) formule un avis sur toute proposition d'amendement à la présente Convention qui lui est soumis conformément à l'article 21, paragraphe 3 ;	c) formule un avis sur toute proposition d'amendement à la présente Convention quilui est soumis conformément à l'article 25, paragraphe 3 ;

d) d peut, à la demande d'une Partie, exprimer un avis sur toute question relative à l'application de la présente Convention.	d) peut exprimer un avis sur toute question relative à l'interprétation ou à l'application de la présente Convention ;
	e) formule, préalablement à toute nouvelle adhésion à la Convention, un avis destiné au Comité des Ministres sur le niveau de protection des données à caractère personnel assuré par le candidat à l'adhésion et recommande, le cas échéant, des mesures à prendre en vue d'atteindre la conformité avec les dispositions de la présente Convention ;
	f) peut, à la demande d'un État ou d'une organisation internationale, évaluer si leur niveau de protection des données à caractère personnel est conforme aux dispositions de la présente Convention et recommande, le cas échéant, des mesures à prendre en vue d'atteindre une telle conformité ;
	g) peut élaborer ou approuver des modèles de garanties standardisées au sens de l'article 14 ;
	h) examine la mise en œuvre de la présente Convention par les Parties et recommande des mesures à prendre en cas de non-respect de la présente Convention par une Partie ;
	i) examine la mise en œuvre de la présente Convention par les Parties et recommande des mesures à prendre en cas de non-respect de la présente Convention par une Partie ;
	facilite au besoin le règlement amiable de toute difficulté d'application de la présente Convention.

Article 20 – Procédure	**Article 24 – Procédure**
1. Le comité consultatif est convoqué par le Secrétaire Général du Conseil de l'Europe. Il tient sa première réunion dans les douze mois qui suivent l'entrée en vigueur de la présente Convention. Il se réunit par la suite au moins une fois tous les deux ans et, en tout cas, chaque fois qu'un tiers des représentants des Parties demande sa convocation.	1. Le Comité conventionnel est convoqué par le Secrétaire Général du Conseil de l'Europe. Il tient sa première réunion dans les douze mois qui suivent l'entrée en vigueur de la présente Convention. Il se réunit par la suite au moins une fois par an et, en tous cas, chaque fois qu'un tiers des représentants des Parties demande sa convocation.
2. La majorité des représentants des Parties constitue le quorum nécessaire pour tenir une réunion du comité consultatif.	Supprimé
3. À l'issue de chacune de ses réunions, le comité consultatif soumet au Comité des Ministres du Conseil de l'Europeun rapport sur ses travaux et sur le fonctionnement de la Convention.	2. À l'issue de chacune de ses réunions, le Comité conventionnel soumet au Comité des Ministres du Conseil de l'Europe un rapport sur ses travaux et sur le fonctionnement de la présente Convention.
	3. Les modalités de vote au sein du Comité conventionnel sont fixées dans les éléments pour le règlement intérieur annexés au Protocole n° STCE [223].
4. Sous réserve des dispositions de la présente Convention, le Comité consultatif établit son règlement intérieur.	4. Le Comité conventionnel établit les autreséléments de son règlement intérieur et fixe en particulier les procédures d'évaluation et d'examen prévues à l'article 4, paragraphe 3 et à l'article 23, alinéas e, f et h sur la base de critères objectifs.
Chapitre VI – Amendements	**Chapitre VII – Amendements**
Article 21 – Amendements	**Article 25 – Amendements**
1. Des amendements à la présente Convention peuvent être proposés par une Partie, par le Comité des Ministres du Conseil de l'Europe ou par le comité consultatif.	1. Des amendements à la présente Convention peuvent être proposés par une Partie, par le Comité des Ministres du Conseil de l'Europe ou par le comité conventionnel.

2. Toute proposition d'amendement est communiquée par le Secrétaire Général du Conseil de l'Europe aux États membres du Conseil de l'Europe et à chaque État non-membre qui a adhéré ou a été invité à adhérer à la présente Convention conformément aux dispositions de l'article 23.	2. Toute proposition d'amendement est communiquée par le Secrétaire Général du Conseil de l'Europe aux Parties à la présente Convention, aux autres États membres du Conseil de l'Europe, à l'Union européenne et à chaque État non-membre ou organisation internationale qui a été invité(e) à adhérer à la présente Convention conformément aux dispositions de l'article 28.
3. En outre, tout amendement proposé par une Partie ou par le Comité des Ministres est communiqué au comité consultatif qui soumet au Comité des Ministres son avis sur l'amendement proposé.	3. En outre, tout amendement proposé par une Partie ou par le Comité des Ministres est communiqué au comité conventionnel, qui soumet au Comité des Ministres son avis sur l'amendement proposé.
4. Le Comité des Ministres examine l'amendement proposé et tout avis soumis par le comité consultatif et peut approuver l'amendement.	4. Le Comité des Ministres examine l'amendement proposé et tout avis soumis par le comité conventionnel, et peut approuver l'amendement.
5. Le texte de tout amendement approuvé par le Comité des Ministres conformément au paragraphe 4 du présent article est transmis aux Parties pour acceptation.	5. Le texte de tout amendement approuvé par le Comité des Ministres conformément au paragraphe 4 du présent article est transmis aux Parties pour acceptation.
6. Tout amendement approuvé conformément au paragraphe 4 du présent article entrera en vigueur le trentième jour après que toutes les Parties auront informé le Secrétaire Général qu'elles l'ont accepté.	6. Tout amendement approuvé conformément au paragraphe 4 du présent article entrera en vigueur le trentième jour après que toutes les Parties auront informé le Secrétaire Général qu'elles l'ont accepté.
	7. Par ailleurs, le Comité des Ministres peut, après consultation du comité conventionnel, décider à l'unanimité qu'un amendement en particulier entrera en vigueur à l'expiration d'une période de trois ans à compter de la date à laquelle il aura été ouvert à l'acceptation, sauf si une Partie a notifié au Secrétaire Général du Conseil de l'Europe une objection à son entrée en vigueur. Lorsqu'une telle objection a été notifiée, l'amendement entrera en vigueur le premier jour du mois suivant la date à laquelle la Partie à la présente Convention qui a notifié l'objection aura déposé son instrument

	d'acceptation auprès du Secrétaire Général du Conseil de l'Europe
Chapitre VII – Clauses finales	**Chapitre VIII – Clauses finales**
Article 22 – Entrée en vigueur	**Article 26 – Entrée en vigueur**
1. La présente Convention est ouverte à la signature des États membres duConseil de l'Europe. Elle sera soumise à ratification, acceptation ou approbation. Les instruments de ratification, d'acceptation ou d'approbation seront déposés près le Secrétaire Général du Conseil de l'Europe.	1. La présente Convention est ouverte à la signature des États membres du Conseil de l'Europe et de l'Union européenne. Elle sera soumise à ratification, acceptation ou approbation. Les instruments de ratification, d'acceptation ou d'approbation seront déposés près le Secrétaire Général du Conseil de l'Europe.
2. La présente Convention entrera en vigueur le premier jour du mois qui suit l'expiration d'une période de trois mois aprèsla date à laquelle cinq États membres du Conseil de l'Europe auront exprimé leur consentement à être liés par la Convention conformément aux dispositions du paragraphe précédent.	2. La présente Convention entrera en vigueur le premier jour du mois qui suit l'expiration d'une période de trois mois après la date à laquelle cinq États membres du Conseil de l'Europe auront exprimé leur consentement à être liés par la Convention conformément aux dispositions du paragraphe précédent.
3. Pour tout État membre qui exprimera ultérieurement son consentement à être lié par la Convention, celle-ci entrera en vigueur le premier jour du mois qui suit l'expiration d'une période de trois mois après la date du dépôt de l'instrument de ratification, d'acceptation ou d'approbation.	3. Pour toute Partie qui exprimera ultérieurement son consentement à être liée par la Convention, cette dernière entrera en vigueur le premier jour du mois qui suit l'expiration d'une période de trois mois après la date du dépôt de l'instrument de ratification, d'acceptation ou d'approbation.
Article23 – Adhésion d'États non membres	**Article 27 – Adhésion d'États non-membres ou d'organisations internationales**

1. Après l'entrée en vigueur de la présente Convention, le Comité des Ministres du Conseil de l'Europe pourra inviter tout État non-membre du Conseil de l'Europe à adhérer à la présente Convention par une décision prise à la majorité prévue à l'article 20.d du Statut du Conseil de l'Europe et à l'unanimité des représentants des États contractants ayant le droit de siéger au comité.	1. Après l'entrée en vigueur de la présente Convention, le Comité des Ministres du Conseil de l'Europe pourra, après consultation des Parties à la présente Convention et en avoir obtenu l'assentiment unanime, et à la lumière de l'avis formulé par le Comité conventionnel conformément à l'article 23.e, inviter tout État non-membre du Conseil de l'Europe ou une organisation internationale à adhérer à la présente Convention par une décision prise à la majorité prévue à l'article 20.d du Statut du Conseil de l'Europe, et à l'unanimité des représentants des États contractants ayant le droit de siéger au Comité des Ministres.
2. Pour tout État adhérant, la Convention entrera en vigueur le premier jour du mois qui suit l'expiration d'une période de trois mois après la date du dépôt de l'instrument d'adhésion près le Secrétaire Général du Conseil de l'Europe.	2. Pour tout État ou organisation internationale adhérant à la présente Convention conformément au paragraphe 1 ci-dessus, la Convention entrera en vigueur le premier jour du mois qui suit l'expiration d'une période de trois mois après la date du dépôt de l'instrument d'adhésion près le Secrétaire Général du Conseil de l'Europe.
Article 24 – Clause territoriale	**Article 28 – Clause territoriale**
1. Tout État peut, au moment de la signature ou au moment du dépôt de son instrument de ratification, d'acceptation, d'approbation ou d'adhésion, désigner le ou les territoires auxquels s'appliquera la présente Convention.	1. Tout État, l'Union européenne ou une autre organisation internationale peuvent, au moment de la signature ou au moment du dépôt de son instrument de ratification, d'acceptation, d'approbation ou d'adhésion, désigner le ou les territoires auxquels s'appliquera la présente Convention.
2. Tout État peut, à tout autre moment par la suite, par une déclaration adressée au Secrétaire Général du Conseil de l'Europe, étendre l'application de la présente Convention à tout autre territoire désigné dans la déclaration. La Convention entrera en vigueur à l'égard de ce territoire le premier jour du mois qui suit l'expiration d'une période de trois mois après la date de réception de la déclaration par le Secrétaire Général.	2. Tout État, l'Union européenne ou une autre organisation internationale peuvent, à tout autre moment par la suite, par une déclaration adressée au Secrétaire Général du Conseil de l'Europe, étendre l'application de la présente Convention à tout autre territoire désigné dans la déclaration. La Convention entrera en vigueur à l'égard de ce territoire le premier jour du mois qui suit l'expiration d'une période de trois mois après la date de réception de la déclaration par le

	Secrétaire Général.
3. Toute déclaration faite en vertu des deux paragraphes précédents pourra être retirée, en ce qui concerne tout territoire désigné dans cette déclaration, par notification adressée au Secrétaire Général. Le retrait prendra effet le premier jour du mois qui suit l'expiration d'une période de six mois après la date de réception de la notification par le Secrétaire Général.	3. Toute déclaration faite en vertu des deux paragraphes précédents pourra êtreretirée, en ce qui concerne tout territoire désigné dans cette déclaration, par notification adressée au Secrétaire Général. Le retrait prendra effet le premier jour du mois qui suit l'expiration d'une période de six mois après la date de réception de la notification par le Secrétaire Général
Article 25 – Réserves	**Article 29 – Réserves**
Aucune réserve n'est admise aux dispositions de la présente Convention.	Aucune réserve n'est admise aux dispositions de la présente Convention.
Article 26 – Dénonciation	**Article 30 – Dénonciation**
1. Toute Partie peut, à tout moment, dénoncer la présente Convention en adressant une notification au Secrétaire Général du Conseil de l'Europe.	1. Toute Partie peut, à tout moment, dénoncer la présente Convention en adressant une notification au Secrétaire Général du Conseil de l'Europe.
2. La dénonciation prendra effet le premier jour du mois qui suit l'expiration d'une période de six mois après la date de réception de la notification par le Secrétaire Général.	2. La dénonciation prendra effet le premier jour du mois qui suit l'expiration d'une période de six mois après la date de réception de la notification par le Secrétaire Général.
Article 27 – Notifications	**Article 31 – Notifications**
Le Secrétaire Général du Conseil de l'Europe notifiera aux États membres du Conseil et à tout État ayant adhéré à la présente Convention :	Le Secrétaire Général du Conseil de l'Europe notifiera aux États membres du Conseil et à toute Partie à la présente Convention :
a) toute signature ;	a) toute signature ;
b) le dépôt de tout instrument de ratification, d'acceptation, d'approbation oud'adhésion ;	b) le dépôt de tout instrument de ratification, d'acceptation, d'approbation ou d'adhésion.
c) toute date d'entrée en vigueur de la présente Convention conformément à ses articles 22, 23 et 24 ;	c) toute date d'entrée en vigueur de la présente Convention conformément à ses articles 26, 27 et 28 ;

d) tout autre acte, notification ou communication ayant trait à la présente Convention.	d) d tout autre acte, notification ou communication ayant trait à la présente Convention.
	Annexe au Protocole : Éléments pour le Règlement intérieur du comité conventionnel
	1. Chaque Partie a le droit de vote et dispose d'une voix.
	2. La majorité des deux tiers des représentants des Parties constitue le quorum nécessaire pour tenir une réunion du comité conventionnel. Dans le cas où le Protocole d'amendement à la Convention entrerait en vigueur conformément à l'article 37 paragraphe 2 avant son entrée en vigueur à l'égard de tous les États contractants à la Convention, le quorum nécessaire pour tenir une réunion du comitéconventionnel sera d'au moins 34 Parties au Protocole.
	3. Les décisions au titre de l'article 23 sont prises à la majorité des quatre cinquièmes. Les décisions au titre de l'article 23, alinéa h sont prises à la majorité des quatre cinquièmes, y compris la majorité des voix des États Parties non-membres d'une organisation d'intégration régionale qui est Partie à la Convention.
	4. Lorsque le comité conventionnel prend des décisions en vertu de l'article 23, alinéa h, la Partie concernée par l'examen ne vote pas. Dès lors qu'une telle décision concerne une question relevant de la compétence d'une organisation d'intégration régionale, ni l'organisation ni ses États membres ne votent.
	5. Les décisions concernant les questions procédurales sont prises à la majorité simple.

	6. Les organisations d'intégration régionale, dans les domaines relevant de leur compétence, peuvent exercer leur droit de vote au sein du comité conventionnelavec un nombre de voix égal au nombre de leurs États membres qui sont Parties à la Convention. Une telle organisation n'exerce pas son droit de vote si l'un de ses États membres exerce son droit.
	7. En cas de vote, toutes les Parties doivent être informées de l'objet et du moment du vote, ainsi que du fait que le vote sera exercé par les Parties individuellement ou par une organisation d'intégration régionale au nom de ses États membres.
	8. Le comité conventionnel peut ultérieurement amender le règlement intérieur à la majorité des deux tiers des Parties, à l’exception des modalités de vote qui ne peuvent être amendées qu’à l’unanimité et auxquelles l’article 25 de la Convention s’applique.

ANNEXE N° 3 : LISTE DES CONTRIBUTIONS ÉCRITES

- Commission nationale de l'informatique et des libertés (CNIL)

- Direction du numérique pour l'éducation (Ministère de l'Éducation nationale et de la Jeunesse)

- Ministère de l'Europe et des affaires étrangères