Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Préposé fédéral à la protection des données et à la transparence
PFPDT

International Conference
Modernisation of Data Protection Legislation in Europe

Hotel Arka, Skopje
30 – 31 May 2012

Modernisation de la Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (Convention 108)

Jean-Philippe Walter, Dr en droit
Préposé fédéral suppléant
Président du Comité consultatif (Convention 108)

I. Introduction

A l'occasion du 30e anniversaire de l'ouverture à la ratification de la Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (Convention 108), le Conseil de l'Europe et le comité consultatif de la Convention 108 ont entamé le processus de modernisation du seul instrument juridique international contraignant. Si les dispositions de la convention et de son protocole additionnel conservent toute leur pertinence eu égard au traitement de données personnelles, des aménagements sont nécessaires pour

Feldeggweg 1, 3003 Berne
Tél. 031 323 74 84, Fax 031 325 99 96
www.edoeb.admin.ch

être mieux en mesure de répondre aux défis que représentent la globalisation, ainsi que les évolutions technologiques, leurs usages multifonctionnels et ubiquistes et leurs effets de masse qui pèsent sur la vie privée et le droit à la protection des données.

La Convention 108 demeure ainsi une excellente base à partir de laquelle il est possible de répondre aux attentes légitimes des personnes concernées et des responsables de traitement tout en renforçant l'effectivité de la protection des données et la mise en œuvre de ses principes fondamentaux. A titre préliminaire permettez moi dès lors de rappeler ici les points forts de la convention 108 et de son protocole additionnel :

- La Convention est le texte de référence de nombreux textes internationaux et nationaux, en commençant par la directive 95/46/CE qui constitue un développement des principes de la Convention.

- Avec le protocole additionnel, il s'agit du premier et seul texte international régissant la protection des données ayant un caractère contraignant. A ce jour, 77 Etats issus des 5 continents ont adopté une loi de protection des données. Plus de la moitié de ces Etats sont partie à la Convention. Celle-ci a en effet été ratifiée par 43 des 47 Etats membres du Conseil de l'Europe, dont les 27 pays membres de l'Union européenne.

- Elle énonce les principes de base de la protection des données qui sont universellement reconnus et ses normes juridiques contraignantes sont parfaitement cohérentes avec d'autres textes comme les lignes directrices de l'OCDE ou plus encore avec les principes directeurs des Nations Unies.

- La Convention est rédigée de manière simple et générale et suit une approche dite « technologiquement neutre » gardant une actualité aux normes juridiques fondamentales qu'elle contient et permettant une adaptation

aux évolutions technologiques sans abaisser le niveau de protection ou exclure une protection renforcée selon les besoins ou les situations.

- Elle est d'application horizontale et couvre l'ensemble des traitements de données automatisés du secteur privé et du secteur public, y compris dans le domaine de la police et de la justice.

- En conciliant le droit au respect de la vie privée et la liberté d'information (notamment le droit à la libre circulation des données sans considération de frontières), elle garantit un haut niveau de protection dans le respect des systèmes juridiques existants et assure en principe la libre circulation des données entre les Etats parties tout en exigeant (au travers du protocole additionnel) un niveau de protection adéquat pour le transfert auprès des pays non parties à la convention.

- La Convention règle la coopération entre les Parties et l'assistance aux personnes concernées quelles que soient leur nationalité ou leur lieu de résidence. Elle met en place une plateforme de coopération multilatérale par le biais du comité consultatif.

- Elaborée avec la participation d'Etats non membres du Conseil de l'Europe (USA, Canada, Australie et Japon), la Convention n'est pas un texte purement européen. Elle est ouverte à l'adhésion d'Etats tiers, ce qui lui donne un potentiel universel.

II. Objectifs de la modernisation

Ces points forts ont servi d'orientation aux travaux en cours, lesquels ont pour objectifs de :

- Gérer les défis de la vie privée qui résultent de l'utilisation des technologies de l'information et des télécommunications ;
- Renforcer le droit à la protection des données en tant que droit fondamental indispensable à l'exercice d'autres droits et libertés fondamentales lors du traitement de données à caractère personnel. Il s'agit en particulier de permettre aux personnes de mieux maîtriser les données qui les concernent et de garantir le respect de la dignité humaine lors du traitement de données personnelles ;
- Concilier le droit à la protection des données avec l'exercice d'autres droits et libertés fondamentales, en particulier avec la liberté d'expression qui acquiert une toute autre dimension dans le monde de l'Internet ;.
- Renforcer les mécanismes de mise en œuvre et de suivi de la convention ;
- Maintenir la nature générale et technologiquement neutre des dispositions de la convention quitte à compléter l'instrument par des textes sectoriels plus détaillés ;
- Assurer la cohérence et la compatibilité avec le cadre juridique de l'Union européenne ;
- Préserver, réaffirmer, renforcer et promouvoir la vocation universelle et le caractère ouvert de la Convention.

Sur la base de ces objectifs, le bureau du comité consultatif prépare un projet[1] qui devrait être adopté par le comité consultatif lors de sa prochaine réunion plénière en juin prochain. Quant à la forme juridique de l'exercice, différentes options sont encore ouvertes, mais on s'achemine vraisemblablement vers un protocole d'amendement de la Convention.

[1] Document T-PD-BUR (2012) 01 Rev_fr, http://www.coe.int/t/dghl/standardsetting/dataprotection/Default_fr.asp

III. Grandes lignes du projet de modernisation

1. Objet et but

A l'article 1, il est proposé de mieux souligner l'objectif de la Convention, à savoir la garantie à toute personne physique relevant de la juridiction d'une Partie, quelle que soit sa nationalité ou sa résidence, du droit à la protection des données à caractère personnel afin d'assurer le respect de ses autres droits et libertés fondamentales, notamment de son droit à la vie privée à l'égard du traitement de ses données. Par cette formulation, la convention ne crée pas une hiérarchie des droits, mais rappelle que le traitement de données à caractère personnel affecte d'autres droits et libertés fondamentales et que leur respect passe par la garantie du droit à la protection des données. Le droit à la protection des données est en lien avec l'ensemble des autres droits et libertés fondamentales et vient en fait les renforcer. Il ne doit pas être par contre considéré comme une prérogative absolue, mais il doit être pris par rapport à sa fonction dans la société[2]. Conformément au principe de proportionnalité, ce droit ne doit pas être exercé de manière à empêcher l'exercice d'autres droits et libertés fondamentales. Il s'agit de concilier les différents droits et libertés en présence.

2. Champ d'application et définitions

Par rapport au texte en vigueur, le projet étend le champ d'application à l'ensemble des traitements automatisés ou non automatisés de données personnelles qui relèvent de la juridiction d'une partie. Il continue de couvrir les traitements dans les secteurs privés et publics, y compris la police et la justice. Il intègre ainsi les traitements manuels, dans la mesure où les données font partie d'un ensemble dont la structure permet selon des critères déterminés de rechercher les données par personne concernée. Actuellement ces traitements ne sont couverts que pour autant qu'un Etat contractant déclare étendre le champ d'application aux données manuelles. A

[2] Voir considérant 139 du projet de règlement européen ; voir arrêts de la CJE, C-92/09 et C-93/09 *Volker et Markus Schecke*[2010] CJE I-0000, §§ 48, 50 et 86

l'instar du règlement européen, même si cela ne ressort pas expressément du texte retenu, l'expression « relevant de sa juridiction » permet de couvrir également les traitements découlant d'activités et de services destinés à des personnes relevant de la juridiction d'une Partie, et aux traitements découlant de l'observation du comportement des personnes concernées, lorsque ces traitements sont opérés par des responsables du traitement ne relevant pas de la juridiction d'une Partie.

Par contre, la Convention ne devrait plus s'appliquer aux traitements de données effectués par une personne physique pour l'exercice d'activités exclusivement personnelles ou domestiques. Dans ce contexte, une attention particulière doit être accordée au phénomène des réseaux sociaux, blogs et autres services internet sur lesquels des informations personnelles sont partagées dans le cadre d'activités purement domestiques. Toutefois les critères de délimitation sont difficiles à établir et pour l'instant, il est proposé d'appliquer pleinement la convention dès lors que des données personnelles sont accessibles à des personnes externes à la sphère personnelle ou domestique. Nous avons également renoncé à étendre l'exception aux responsables de traitement ou aux sous traitants qui fournissent les moyens de traiter des données à caractère personnel pour de telles activités personnelles ou domestiques.

Quant aux définitions, elles subiront un toilettage. Tout d'abord l'exposé des motifs précisera la notion de « personne identifiable ». Ainsi une personne n'est pas identifiable si cette identification nécessite des délais ou des activités déraisonnables pour le responsable du traitement ou pour toute personne auprès de qui le responsable du traitement pourrait raisonnablement obtenir l'identification. Par « identifiable », on ne se réfère pas seulement aux éléments de l'identité civile d'un individu, mais aussi à ce qui permet d'individualiser une personne parmi d'autres.

En outre, la notion de fichier sera abandonné. Celle de maître du fichier sera remplacée par la notion de responsable de traitement, laquelle sera complétée par les notions de sous-traitant et de destinataire des données. Contrairement au projet euro-

péen, nous n'avons pas retenu les définitions de données génétiques et de données biométriques, car nous estimons que ces notions sont évolutives et qu'il est prématuré de les fixer dans un texte juridique. Elles seront développés dans l'exposé des motifs.

3. Engagement des parties

La Convention n'est pas d'application directe. Aux termes de l'article 4, chaque Partie prend, dans son droit interne, les mesures nécessaires pour donner effet aux dispositions de la Convention. Cela doit être fait au plus tard au moment de l'entrée en vigueur de la Convention. Il n'y a actuellement aucun contrôle pour vérifier si ces mesures ont été réellement prises et sont effectives. Nous proposons à l'avenir d'une part d'exiger que ces mesures soient prises avant la ratification ou l'adhésion à la Convention. D'autre part le « candidat » à l'adhésion ou à la ratification devra démontrer que les mesures prises ont été prises et qu'elles sont effectives. En ratifiant ou en adhérant à la convention, les Parties acceptent en effet que le comité conventionnel puisse évaluer le respect de leurs engagements. Elles doivent en outre contribuer activement à cette évaluation..

4. Principes de base

En ce qui concerne les principes de base de la protection des données, les principes actuels de l'article 5 sont en soi suffisants pour couvrir les différentes situations du traitement de données personnelles. Néanmoins, nous proposons de renforcer le texte en complétant le principe de proportionnalité de l'article 5, lettre c qui vise essentiellement les données, lesquelles doivent être adéquates, pertinentes et non excessives par rapport aux finalités pour lesquelles elles sont enregistrées. Le principe de proportionnalité cependant doit également concerner le traitement et en particulier le choix des moyens et les méthodes de traitement. Ainsi, le traitement doit être proportionné, c.à.d. apte et nécessaire à atteindre la finalité légitime poursuivie et refléter un juste équilibre entre les intérêts publics ou privés, les droits et libertés fonda-

mentales qui sont en jeu. Ce principe est également complété par le principe de la minimisation des données selon lequel la collecte et le traitement doivent être limitées au strict minimum nécessaire.

Actuellement, la Convention ne prévoit pas de motifs légitimant le traitement. Elle prévoit simplement et de manière générale que tout traitement de données doit être licite. Nous proposons d'introduire une nouvelle disposition qui prévoit que le traitement de données ne peut intervenir que si la personne concernée a donné son consentement de manière spécifique, explicite, libre et éclairé ou si le traitement est prévu par le droit interne pour un intérêt légitime prépondérant ou est nécessaire au respect d'une obligation légale ou d'une obligation contractuelle qui lierait la personne concernée. Afin de préserver la souplesse et le caractère général de la convention, nous avons renoncé à énoncer de manière plus détaillée les motifs de légitimation du traitement, comme le fait la directive européenne 95/46/CE, estimant que les motifs généraux retenus couvrent les situations prévues par la réglementation européenne. Concernant le consentement lorsqu'il est requis, il devrait être explicite, quelle que soit la nature des données traitées. Ce renforcement est justifié par le fait qu'il semble nécessaire, notamment dans le monde virtuel, de dissiper toute ambiguïté quant à la validité du consentement exprimée, ce qui est d'autant plus important dans les opérations de traitement effectuées en ligne. Ainsi le consentement explicite requiert une action positive et affirmative de la personne concernée. Cela ne nécessite pas un consentement écrit : « les responsables du traitement sont … encouragés à mettre en place des procédures et des mécanismes ne laissant aucun doute sur l'octroi du consentement, que ce soit par une action explicite de la personne concernée ou par une déduction claire d'une action effectuée par la personne concernée » [3] Ce renforcement ne fait cependant pas l'unanimité et il n'est pas certain qu'il soit maintenu. Enfin, le consentement doit, dans les limites du principe de la bonne foi, pouvoir être retiré.

[3] Avis 15/2011 du Groupe de l'article 29 du 13 juillet 2011 sur la définition du consentement , p. 28

5. Données sensibles

Concernant les données sensibles, le principe de l'interdiction en l'absence de garanties appropriées du droit interne sera maintenue. Nous proposons néanmoins de revoir le catalogue des données sensibles en y ajoutant les données génétiques et biométriques, les données relatives à l'appartenance syndicale et au côté des condamnations pénales, celles concernant les infractions et les autres mesures de caractère pénal. La disposition fait en outre une distinction entre les données sensibles par nature (par exemple données de santé, données génétiques) et celles qui le deviennent du fait de leur utilisation, par exemple les données dont le traitement révèle l'origine raciale ou les opinions politiques. Dans cette deuxième catégorie, on met l'accent sur la fonction du traitement. Ainsi le fait de conserver une photo dans un fichier n'est pas nécessairement sensible si l'objectif du traitement n'est pas de déduire des informations découlant de l'analyse de la photo. La disposition qualifie également de sensible les données qui du fait de leur traitement présente un risque grave pour les intérêts, les droits et les libertés fondamentales de la personne concernée, notamment un risque de discrimination. Cette dernière ouverture permet de considérer certains traitements comme sensibles, non seulement sur la base de la nature des données, mais également en tenant compte de la finalité et des circonstances du traitement.

6. Sécurité des données

Au niveau de la sécurité des données, le projet prévoit d'introduire l'obligation d'annoncer les violations des données. Cette obligation se limite cependant à des cas significatifs, c.à.d. les violations qui sont susceptibles de porter gravement atteintes aux droits et libertés fondamentales. L'annonce doit être faite aux autorités de contrôle. Contrairement au projet de règlement européen, le projet ne prévoit pas d'obligation d'informer les personnes concernées. Toutefois dans l'exposé des motifs, les responsables de traitement seront encouragés à le faire en cas de risques graves. En outre, les autorités de contrôle pourront, dans le cadre de leur compéten-

ce, inviter les responsables de traitement à le faire. Cette solution laisse une marge de manœuvre pour tenir compte de la particularité de chaque situation.

7. Transparence des traitements

Le projet introduit l'obligation de garantir la transparence des traitements. Le responsable du traitement devra fournir un minimum d'informations, notamment relatives à son identité et à sa résidence habituelle ou son lieu d'établissement, sur les finalités du traitement qu'il effectue, sur les destinataires de données, sur la durée de conservation et sur les moyens d'exercer les droits des personnes concernées. Au besoin, il devra fournir des informations complémentaires si elles sont nécessaires pour garantir un traitement loyal des données. Il s'agit par exemple d'informations concernant les transferts éventuels vers des pays tiers ou celles relatives au caractère obligatoire ou facultatif d'une collecte de données. Contrairement au droit de l'Union européenne et dans la logique du caractère général de la convention, le projet ne précise pas le moment auquel l'information doit être donnée. Toutefois pour permettre aux personnes d'agir en connaissance de cause et de faire valoir leur droit ou de donner un consentement valide lorsqu'il est requis, l'information doit être donné le plutôt possible, soit au moment de la collecte des données, soit, si les données ne sont pas collectées auprès des personnes concernées, au moment de leur enregistrement ou dans un délai raisonnable, mais au plus tard lors de leur première communication. La manière d'informer dépendra ainsi des circonstances du traitement ; l'information sera donnée de manière raisonnable. En particulier, il n'y a pas lieu d'informer si la personne est déjà en possession de l'information et que les circonstances du traitement n'ont pas changées. Le responsable du traitement ne sera pas tenu de fournir ces informations lorsque cela lui est impossible (matériellement ou juridiquement) ou implique des efforts disproportionnés. Des exceptions au devoir d'information sont également possibles aux conditions prévues à l'article 9 de la Convention, à savoir notamment pour des motifs liés à la protection de la sûreté de l'Etat ou à la prévention et à la répression des infractions pénales.

8. Droits des personnes concernées

En ce qui concerne les droits des personnes concernées, ils seront également renforcés pour permettre aux personnes de mieux assurer la maitrise sur leurs données et garantir le respect du droit à la dignité humaine et à la non discrimination.

8.1. Droit d'accès et autres droits

Au niveau du droit d'accès, le projet prévoit d'étendre le catalogue des informations à transmettre à la personne concernée lorsqu'elle exerce ce droit. En plus des informations que le responsable du traitement doit donner sous l'angle de la transparence, il devra fournir des informations sur l'origine des données. En outre, la personne concernée sera en droit d'obtenir connaissance du raisonnement qui sous-tend le traitement de données dont les résultats lui sont opposés ou appliqués. Ce nouveau droit est particulièrement important en matière de profilage des individus qui intervient en règle générale de manière automatisée[4]. Il est à relier avec un autre nouveau droit, celui de ne pas être soumis à une décision affectant de manière significative la personne concernée ou produisant des effets juridiques à son égard, lorsque cette décision est prise uniquement sur le fondement d'un traitement automatisé de données, sans que la personne concernée puisse faire valoir son point de vue.

Le projet prévoit également d'introduire expressément dans la Convention un droit de s'opposer à tout moment pour des raisons légitimes à ce que des données à caractère personnel la concernant fassent l'objet d'un traitement. Nous avons par contre renoncé à introduire expressément un droit à l'oubli, notamment un droit à l'oubli numérique. Nous estimons en effet que les garanties existantes (durée de conserva-

[4] Voir à ce sujet, la recommandation (2010) 13 du Comité des Ministres sur la protection des personnes à l'égard du traitement automatisé des données à caractère personnel dans le cadre du profilage et son exposé des motifs, https://wcd.coe.int/ViewDoc.jsp?Ref=CM/Rec%282010%2913&Language=lanFrench&Ver=original&Site=CM&BackColorInternet=C3C3C3&BackColorIntranet=EDB021&BackColorLogged=F5D383

tion des données, droit de rectification ou d'effacement des données) associées au droit d'opposition offrent une protection suffisante.

8.2. Restrictions

Rappelons que ces droits ne sont pas absolus et qu'aux termes de l'article 9 de la Convention, ils peuvent être restreints lorsque cela est prévu par la loi et constitue une mesure nécessaire dans une société démocratique :
- à la protection de la sûreté de l'Etat, à la sécurité publique, à des intérêts économiques et financiers importants de l'Etat ou à la prévention et à la répression des infractions pénales ;
- à la protection de la personne concernée et des droits et libertés d'autrui, notamment la liberté d'expression et d'information. Sont aussi couverts le secret des communications, ainsi que le secret des affaires, les secrets commerciaux et autres secrets protégés par la loi.

Des restrictions sont aussi envisageables pour les traitements de données utilisés à des fins statistiques ou de recherches scientifiques pour autant qu'il n'existe manifestement pas de risques d'atteinte aux droits et libertés des personnes concernées. Enfin les dérogations au titre de l'article 9 visent non seulement l'exercice des droits des personnes concernées, mais également certains principes de base et le devoir d'information.

9. Obligations en matière de protection des données

La révision de la Convention doit également permettre de renforcer les responsabilités de ceux qui traitent ou font traiter des données. Le projet pose ainsi le principe selon lequel le responsable du traitement a la charge de respecter le droit à la protection des données durant toutes les phases du traitement et de prendre toutes les mesures appropriées – y compris en cas de sous-traitance – pour mettre en œuvre les dispositions de protection des données. Cette responsabilité couvre aussi le

choix des moyens utilisés pour le traitement, en particulier il faut recourir à des technologies garantissant le respect des droits et libertés fondamentales. Il introduit également l'obligation du responsable de traitement ou du sous-traitant de procéder à une analyse de l'impact potentiel du traitement envisagé sur les droits et les libertés des individus. Le responsable du traitement devra en outre concevoir les traitements de données de manière à prévenir ou pour le moins à minimiser les risques d'atteinte au droit de la protection des données. Il devra mettre en place des mécanismes internes permettant de démontrer aux personnes concernées et aux autorités de protection des données la conformité des traitements avec les dispositions de protection des données qui lui sont applicables. Parmi ces mesures, on pense en particulier à la nomination d'un délégué à la protection des données. Ces exigences faites au responsable de traitement devront être modulées en fonction de la taille de l'entreprise, du volume des données traitées, de leur sensibilité et des risques que ces traitements peuvent entrainer pour les personnes concernées. Enfin, nous proposons d'introduire une exigence selon laquelle les produits et les services destinés au traitement de données à caractère personnel et diffusés sur ou à partir de la juridiction d'une Partie, devraient comporter des fonctionnalités simples d'usage et permettant d'assurer la conformité des traitements de données au regard du droit applicable. Ces obligations et en particulier l'analyse d'impact, laquelle doit être envisagée pour tout traitement de données à caractère personnel, doivent être proportionnées aux risques potentiels pour les intérêts, les droits et les libertés fondamentales des personnes concernées. Elles doivent notamment tenir compte de la nature du traitement, de la grandeur de l'entreprise (responsable de traitement, sous-traitant), du volume des données traitées, du nombre ou catégories de personnes concernées, ainsi que des technologies utilisées.

10. Flux transfrontières de données

Au niveau des flux transfrontières de données, la réglementation proposée permet de préciser la notion de flux transfrontières, à savoir le fait de communiquer ou de rendre accessibles des données en dehors de la juridiction à laquelle celui ou celle qui communique, est soumis. Cette définition englobe également la diffusion de données via Internet. Il ne parait en effet pas illégitime de soumettre à la protection du régime des flux les données mises sur Internet, lorsqu'on mesure la perte de maîtrise qui peut découler de leur publication via ce canal et les risques élevés qui peuvent en découler. Le projet se base sur la notion de niveau adéquat de protection. Le principe de la libre circulation des données entre Parties à la Convention est maintenu : le projet présume en effet un niveau de protection des données adéquat dès lors qu'un Etat ou une organisation internationale a ratifié ou adhéré à la Convention pour autant que les droits et les obligations découlant de la Convention aient été effectivement mis en œuvre. Le comité conventionnel pourra le cas échéant constater que le niveau de protection est insuffisant.

Lorsque le destinataire ne relève pas de la juridiction d'une Partie à la Convention, le transfert ne peut, en règle générale, intervenir que si un niveau de protection adéquat est garanti. Ce niveau peut être assuré par les règles de droit régissant le destinataire, par exemple l'existence d'une législation de protection des données. Il peut découler de mesures juridiques standardisées ou ad 'hoc telles que des clauses contractuelles, des règles internes ou des mesures similaires, contraignantes, effectives et susceptibles de recours effectifs, mises en œuvre par la personne qui communique ou rend accessible les données ou par le destinataire. Le projet prévoit que les autorités de protection des données doivent être informées des mesures prises. Elles pourront exiger que l'effectivité et la qualité de ces mesures leur soient démontrées. Le cas échéant, elles pourront suspendre, interdire ou soumettre à condition le transfert ; elles pourront également exiger de revoir les mesures encadrant le dit transfert.

En l’absence d’un niveau de protection des données adéquat, la communication ou la mise à disposition des données est également possible à certaines conditions. Le transfert peut avoir lieu avec le consentement de la personne concernée. Elle doit avoir au préalable été informée des risques dus à l’absence de garanties appropriées. Le transfert peut aussi intervenir si les intérêts spécifiques de la personne concernée le nécessitent, par exemple pour la sauvegarde de ses intérêts vitaux. Il peut aussi avoir lieu si des intérêts légitimes protégés par la loi l’exigent. Il s’agit en particulier des intérêts visés à l’article 9 de la Convention. On pense notamment au nécessité de la coopération policière ou judiciaire en matière pénale. Ces transferts en l’absence d’un niveau de protection adéquat ne doivent pas intervenir de manière régulière, mais couvrir des situations particulières. L’autorité de contrôle peut également suspendre, interdire ou soumettre à condition ce type de communication des données ou de mise à disposition intervenant en l’absence d’un niveau de protection adéquat.

Le projet introduit une faculté pour les Parties de déroger par des mesures législatives aux dispositions régissant les flux transfrontières de données lorsque ces dérogations constituent une mesure nécessaire dans une société démocratique à la protection de la liberté d’expression et d’information. De telles dérogations peuvent s’avérer nécessaires notamment dans le contexte de la diffusion des données sur Internet liées à l’exercice de ces deux libertés fondamentales.

La question cruciale dans le cadre des flux transfrontières est celle de savoir comment sera déterminé le niveau adéquat et comment pourra-t-on faire converger et coordonner la procédure d’adéquation au sein de l’Union européenne avec les évaluations qui devront être menées au Conseil de l’Europe. L’attrait pour la Convention 108 pour les Etats tiers dépendra également de la reconnaissance de l’adéquation pour pouvoir bénéficier de la libre circulation des informations avec les pays membres de l’Union européenne. Il est dès lors important que les exigences d’adéquation soient les mêmes à Bruxelles qu’à Strasbourg et qu’un mécanisme de suivi soit mis en place dans le cadre de la Convention. Les critères définis par le groupe de l’article

29[5] pour une reconnaissance d'adéquation rejoignent largement les principes définis dans la Convention et sont certainement une bonne base pour les travaux qui seront menés par le comité consultatif.

11. Autorités de contrôle

Le projet de modernisation aborde également la question des autorités de contrôle. Reprenant l'article 1 du protocole additionnel, le projet complète le catalogue des compétences des autorités en prévoyant, en plus des pouvoirs d'intervention, d'investigation, d'ester en justice ou de porter à la connaissance de l'autorité judiciaire les violations des disposition de la protection des données, un devoir de sensibilisation, d'information et d'éducation des acteurs impliqués (personnes concernées, responsable de traitement, sous-traitant, etc.). Il prévoit également la possibilité pour les autorités de prendre des décisions et de prononcer des sanctions. Le projet précise en outre l'indépendance dont doit bénéficier l'autorité de contrôle dans l'exercice de ces tâches et de ces pouvoirs. En particulier, ces autorités ne doivent pas être l'objet d'instructions que ce soit des autorités de nomination ou de toutes autres entités. En outre, elles doivent disposer de ressources humaines, techniques et financières adéquates et des infrastructures nécessaires à pouvoir accomplir leurs tâches et exercer leurs pouvoirs de manière effective. Le projet met également l'accent sur la coopération entre autorités de contrôle. Celles-ci doivent coopérer dans la mesure nécessaire à l'accomplissement de leurs tâches, notamment en échangeant des informations relatives à des traitements effectués sur leur territoire ou concernant leur droit et leur pratique administrative en matière de protection des données. La coopération doit aussi porter sur la coordination de leurs investigations ou de leurs interventions, ainsi que sur la conduite d'actions conjointes. Le projet prévoit que pour faciliter cette coordination, les autorités de contrôle peuvent se constituer en conférence. Afin d'éviter de créer de nouvelle structure, la conférence européenne pourrait à l'avenir assumer ce rôle de coordination. La coopération entre les Parties qui est

[5] Document de travail 12 du 24 juillet 1998 « transferts de données personnelles vers des pays tiers : application des articles 25 et 26 de la directive relative à la protection des données. »

déjà prévue actuellement aux articles 13 et suivants de la Convention incombera à l'avenir aux autorités de contrôle. Il en va de même de l'assistance aux personnes pour l'exercice de leurs droits. Enfin, une clarification a été apportée en ce qui concerne les traitements des instances judiciaires. L'autorité de contrôle ne doit pas interférer dans l'indépendance de la justice et n'est dès lors pas compétente pour les traitements effectués par les instances judiciaires dans l'exercice de leurs fonctions juridictionnelles. Par contre, elle l'est pour les autres traitements.

12. Comité conventionnel

La convention met en place un comité consultatif afin de faciliter ou d'améliorer l'application de la convention. Ce comité joue un rôle fondamental dans l'interprétation de la convention, l'échange d'information entre les Parties et le développement du droit de la protection des données. Le projet prévoit de renforcer le rôle et les compétences de ce comité. Il ne sera plus seulement consultatif, mais aura des compétences d'évaluation et de suivi. Dès lors, il est proposé d'en modifier la dénomination. Il devrait être à l'avenir le comité conventionnel. Il pourra en particulier émettre des avis préalable à l'adhésion à la Convention sur le niveau de protection des données offert par l'Etat ou l'organisation internationale concernée. Il pourra également procéder à l'évaluation de la conformité des règles du droit interne régissant cette Partie et vérifier l'effectivité des mesures prises (existence d'une autorité de contrôle, compétence, existence de recours effectifs), en particulier pour vérifier le niveau d'adéquation. Il pourra également évaluer si les normes juridiques devant régir le transfert de données offrent des garanties suffisantes pour assurer un niveau de protection des données adéquat. Pour apprécier le niveau d'adéquation, il devra fixer dans son règlement intérieur la procédure d'examen. Il pourra en outre élaborer des modèles de mesures juridiques standardisées. Enfin, il devra jouer un rôle de facilitateur à la résolution à l'amiable de difficultés surgissant dans l'application de la Convention.

IV. Conclusion

Ce travail de modernisation de la convention fait partie des priorités du comité consultatif et du Conseil de l'Europe. Le projet devrait être avalisé par le comité consultatif lors de sa 28e réunion qui aura lieu du 19 au 22 juin prochain à Strasbourg. Il sera ensuite transmis au comité des Ministres qui chargera un comité ad'hoc d'examiner et de finaliser le projet. Ce comité sera ouvert aux Etats tiers non membres du Conseil de l'Europe qui sont susceptibles d'adhérer à la Convention. Le Conseil de l'Europe tient ainsi à développer le caractère universel et ouvert de la Convention. En favorisant, l'adhésion d'Etat tiers, il renforce la protection des données dans le monde tout en permettant l'échange de données et la coopération entre les Parties.

Avec cette modernisation, la convention gagnera en cohérence avec le droit de l'Union européenne. Elle permettra d'accroître l'effectivité de la protection des données notamment en mettant en place un mécanisme de vérification de la conformité du droit interne des Parties aux dispositions de la Convention et en permettant de procéder à des évaluations de la mise en œuvre. Plus que jamais la Convention est appelé à jouer un rôle fondamental et central dans le développement d'un droit universel à la protection des données. Elle constitue une base solide vers une réglementation universelle en matière de protection des données et offrent aux Etats tiers en y adhérant une opportunité de se voir reconnaître adéquat.