



8. Datenschutztag

Modernisierung und Rolle der Datenschutzkonvention des Europarates

Freitag, 24. Jänner 2014, Wien

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 30^e 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), célébré le 28 janvier 2011 à l'occasion de la journée de la protection des données, 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 qui existe en la matière. 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 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 dont les données font l'objet d'un traitement et des responsables de ce 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 et stipule précisément à cet égard dans son préambule qu'elle précise et amplifie les principes de la Convention et stipule précisément à cet égard dans son préambule qu'elle précise et amplifie les principes de la Convention.
- Avec son protocole additionnel, la Convention est le premier et demeure le seul texte international régissant de façon juridiquement contraignante la protection des données. A ce jour, quelques 80 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 46 Etats de par le monde, dont 45 des 47 Etats membres du Conseil de l'Europe, les 28 pays membres de l'Union européenne inclus.
- Elle énonce les principes de base de la protection des données qui sont universellement reconnus et ses normes juridiques contraignantes sont parfaites.



tement 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, de la justice ou des services de renseignements.
- 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. Depuis août 2013, l'Uruguay est ainsi devenu le



premier Etat non membre du Conseil de l'Europe à avoir adhéré à la Convention et à son protocole additionnel. Le Maroc devrait suivre sous peu.

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 et avec le droit d'accès aux documents officiels ;
- 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 et les autres instruments internationaux en la matière ;
- 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 a préparé un projet qui a été adopté par le comité consultatif lors de sa 29e réunion plénière en novembre 2012¹. Ce projet est en cours d'examen par un comité ad'hoc intergouvernemental (CAHDATA) qui doit finaliser le texte et préparer un protocole d'amendement à la Convention.

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. Ce droit est en lien avec l'ensemble des autres droits et libertés fondamentales et vient en fait les renforcer. Il est ainsi le socle sur lequel repose l'ensemble des droits et des libertés fondamentales touchés par le traitement des données à caractère personnel. Il ne doit pas être par contre considéré comme une prérogative absolue, mais il doit être pris par rapport à sa fonction dans la société². 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.

¹ http://www.coe.int/t/dghl/standardsetting/dataprotection/TPD_documents/TPD_PD%282012%2904Rev4_F_Convention%20108%20modernis%C3%A9e%20version%20F.pdf

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



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, la justice, l'armée et les services de renseignement. 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. Les traitements de données effectués par des responsables de traitement relèvent de la juridiction d'une Partie lorsqu'ils présentent un lien suffisant avec le territoire de cette Partie. A l'instar du projet de 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 (par exemple analyse de comportements) et de services destinés à des personnes établies sur le territoire d'une Partie lorsque ces traitements sont opérés par des responsables du traitement ne relevant pas de la juridiction d'une Partie à la Convention.

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. Cette exclusion veut éviter d'imposer des obligations déraisonnables aux personnes physiques qui traitent des données dans le cadre de leur sphère personnelle sans visées commerciales ou professionnelles. Il s'agit d'activités domestiques comme le stockage d'images, la gestion de la liste des amis ou des membres de la famille, la correspondance, etc. 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. Selon une jurisprudence récente de la haute cour du canton de Zurich, une publication sur Facebook même limitée à son cercle d'amis est à considérer comme publique. Selon la jurisprudence, doit être considéré comme public tout ce qui n'est pas effectué dans le cadre privé. Une assertion ou une opinion est d'ordre privé si elle s'adresse à son cadre familial ou à un cercle d'amis. Il en va de même si elle s'adresse à un cercle relevant de rapports personnels ou offrant un rapport de confiance particulier.³ La publication sur le réseau social n'offre pas ces garanties. L'exception proposée ne s'étend pas 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.

La Convention ne permet pas de réserves. Elle permet cependant aux Parties, par le biais d'une déclaration faite au Secrétariat général du Conseil de l'Europe, de soustraire du champ d'application de la Convention certaines catégories de fichiers automatisés de données à caractère personnel. Cette faculté laissée aux Parties ne doit pas être interprétée comme une façon déguisée d'introduire des réserves. Il s'agit plutôt de permettre aux Etats de mettre entre parenthèse la convention pour des traitements qui n'étaient pas encore soumis à des règles de protection des données au moment de la ratification, mais qui le seront ultérieurement. Il ne peut s'agir d'une exception durable. Le comité propose de biffer à l'avenir cette possibilité de déclaration qui avait son sens dans les années 80, mais qui ne se justifie plus aujourd'hui.

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. Tel est le cas notam-

³ Tagesanzeiger vom 26.11.2013



ment, d'un numéro d'identification, de données de localisation, d'identifiant en ligne (par exemple l'adresse IP) ou d'autres éléments propres à son identité physique, physiologique, génétique, ou psychique.

En outre, la notion de fichier sera abandonnée. 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 de l'Union européenne, le comité consultatif n'a pas retenu les définitions de données génétiques et de données biométriques, car il estimait, à mon sens à juste titre, que ces notions sont évolutives. Il était dès lors prématuré de les fixer dans un texte juridique. Il n'est cependant pas exclu que le CAHDATA introduise ces deux définitions, notamment en s'inspirant des travaux du comité du Conseil de l'Europe sur la bioéthique.

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. Le comité consultatif propose 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 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. Il s'agit là d'un progrès important pour renforcer l'effectivité de la protection des données et l'engagement des Parties à respecter leurs obligations conventionnelles.



4. Principes de base

L'article 5 de la Convention énonce les principes de base de la protection des données, que sont les principes de licéité et de la bonne foi, les principes de finalité et de proportionnalité, ainsi que le principe d'exactitude. Ces principes fondamentaux sont en soi suffisants pour couvrir les différentes situations du traitement de données personnelles. Néanmoins, le comité consultatif estime nécessaire de renforcer le texte en complétant le principe de proportionnalité de l'article 5, lettre c. Cette disposition 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 en présence, ainsi que les droits et libertés fondamentales qui sont en jeu. Il convient en particulier de choisir les moyens de traitement les moins attentatoires aux droits et libertés fondamentales. Ce principe doit être respecté à toutes les étapes du traitement. 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. Le projet introduit 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, libre et éclairé ou si le traitement repose sur un autre fondement légitime prévu par la loi. Afin de préserver la souplesse et le caractère général de la convention, le projet n'énonce pas plus en détails ce qui constitue un fondement légitime. Cette expression couvre en tous les cas les motifs énoncés à l'article 7 de la directive européenne 95/46/CE. Il s'agit en particulier des cas où le traitement est nécessaire à l'exécution d'un contrat (ou de mesures précontractuelles), à la protec-



tion d'intérêts vitaux de la personne concernée, ou encore est justifié par des intérêts légitimes prépondérants.

Concernant le consentement lorsqu'il est requis, il devrait, selon moi, être pour le moins non équivoque, 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, pour être valablement donné, requiert une action positive et affirmative de la personne concernée. Cela ne nécessite pas un consentement écrit : il en découle que « 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 »⁴. L'introduction d'une exigence d'un consentement explicite est encore ouverte et ne fait cependant pas l'unanimité. Un compromis pourrait cependant se faire autour de la notion de consentement non équivoque ou non ambiguë. Enfin, le consentement doit, dans les limites du principe de la bonne foi, pouvoir être retiré en tout temps.

5. Données sensibles

Concernant les données sensibles, le principe de l'interdiction en l'absence de garanties appropriées du droit interne sera maintenu. Le projet précise les contours des garanties à apporter. Ces garanties doivent ainsi avoir pour objectif de prévenir les risques que le traitement de données sensibles peut présenter pour les intérêts, les droits et libertés fondamentales de la personne concernée, et notamment un risque de discrimination.

Le projet revoit le catalogue des données sensibles en y ajoutant les données génétiques et biométriques, les données relatives à l'appartenance syndicale et au côté

⁴ Avis 15/2011 du Groupe de l'article 29 du 13 juillet 2011 sur la définition du consentement , p. 28



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, les 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. Une proposition tendant à qualifier également de sensibles, 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, n'a pas été retenue. Cette proposition permettait 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. Elle introduisait cependant une certaine insécurité juridique. Il convient par ailleurs de noter que par le biais de l'article 11 de la Convention, une Partie peut étendre la liste des données sensibles à d'autres données dont le traitement est susceptible de présenter un risque accru pour les personnes concernées.

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 va moins loin que le projet de règlement européen en se limitant à des cas significatifs, c.à.d. des violations qui sont susceptibles de porter gravement atteinte aux droits et libertés fondamentales des personnes concernées. L'annonce doit être faite au moins aux autorités de contrôle en matière de protection des données. Contrairement au projet de règlement européen, le projet du T-PD ne prévoit pas d'obligation d'informer également les personnes concernées. Toutefois l'exposé des motifs incitera les responsables de traitement à le faire au moins dans les cas les plus graves. En outre, les autorités de contrôle pourront, dans le cadre de leur compétence, 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 donnée 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 activement sous tout format approprié, par exemple par le biais d'un site web, d'outils technologiques sur les dispositifs personnels, par une lettre d'information, etc. L'information sera en outre donnée de manière raisonnable. Elle peut se faire de manière générale ou de manière individuelle selon les circonstances ou la nature du traitement. 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 changé. Lors de collecte auprès de tiers, le responsable du traitement ne sera pas tenu de fournir ces informations lorsque le traitement est expressément prévu par la loi ; dans ce cas, la loi doit être précise et suffisamment détaillée. Le responsable de



traitement ne sera également pas tenu d'informer 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 maîtrise 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 automatisée⁵. 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.

⁵ 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> .



Le projet prévoit également d'introduire expressément dans la Convention un droit de s'opposer à tout moment 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 prépondérants justifiant le traitement. Ces motifs doivent prévaloir sur les intérêts, les droits et sur les libertés fondamentales de la personne concernée. Le comité a par contre renoncé à introduire expressément un droit à l'oubli, notamment un droit à l'oubli numérique. Il estime en effet que les garanties existantes (durée de conservation des données, droit de rectification ou d'effacement des données) associées au droit d'opposition offrent une protection suffisante. Enfin, la personne concernée doit pouvoir disposer d'un recours si les droits qui lui sont octroyés ne sont pas respectés et pouvoir compter sur l'assistance des autorités de protection des données.

8.2. Restrictions

Rappelons que ces droits des personnes concernées 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 national, à la sûreté 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.

Rappelons que la Convention 108 ne prévoit pas la possibilité d'émettre des réserves et qu'en soi elle s'applique à tous les domaines dans lesquels des traitements de données à caractère personnel sont effectués. Avec l'article 9, elle permet cependant de déroger à certaines dispositions lorsque cela est nécessaire dans une société démocratique pour les objectifs mentionnés ci-dessus et pour autant que cela soit prévu par une loi accessible et prévisible. Il ne s'agit pas de mettre entre parenthèse la Convention et par là d'introduire des réserves déguisées, mais d'aménager ou de restreindre certains des principes ou de limiter certains droits pour permettre de mener certaines activités légitimes répondant à un besoin impérieux qui ne peuvent être réalisées sans une intrusion plus grande dans les droits et libertés fondamentales. Il est à noter que contrairement au texte en vigueur, il n'est plus possible de prévoir des dérogations à l'article 6 régissant les données sensibles. En outre, des réflexions sont encore en cours pour voir dans quelle mesure il est admissible de tolérer des dérogations aux principes de base que sont notamment la licéité, la bonne foi, la proportionnalité ou la finalité. On évolue plutôt vers une norme permettant d'aménager ces principes en fonction du secteur concerné.

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 par exemple à la nomination d'un délégué à la protection des données.

Enfin, nous proposons d'introduire une exigence selon laquelle les produits et les services destinés au traitement de données à caractère personnel devraient prendre en compte les implications du droit à la protection des données dès leur conception et faciliter 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 et des données, du nombre ou catégories de personnes concernées, ainsi que des technologies utilisées. La grandeur de l'entreprise (responsable de traitement, sous-traitant) ou le volume des données traitées peuvent également, dans une certaine mesure, être pris en considération.

10. Flux transfrontières de données

L'article 12 du projet de modernisation qui régit les flux transfrontières de données combine l'article 12 de l'actuelle Convention et l'article 2 du protocole additionnel. Il s'agit d'une disposition centrale de la Convention dont l'objectif est d'une part de permettre en principe la libre circulation des informations entre les Parties à la Convention, dans la mesure où elles assurent un haut niveau de protection des données en ayant pris dans leur droit interne les mesures nécessaires à donner effet aux



dispositions de la Convention. D'autre part, il fixe les règles à respecter lors du transfert de données vers des destinataires ne relevant pas de la juridiction d'une Partie à la Convention afin d'assurer une protection appropriée des personnes à l'égard du traitement de données à caractère personnel. Malheureusement le projet ne définit pas le flux transfrontière, se limitant à parler de transfert de données vers un destinataire d'une autre juridiction que celle d'où parte les données. Il laisse ainsi sans réponse claire la question de savoir si le transfert couvre le fait de communiquer ou de rendre accessible des données en dehors de la juridiction à laquelle celui ou celle qui communique, est soumis. Cela laisse ouvert la question de savoir si le transfert englobe également la diffusion de données via Internet. Il ne paraîtrait 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. L'article 12 par contre régit uniquement l'exportation des données et non leur importation.

Le projet reprend la règle de l'article 12 actuel selon laquelle le transfert de données à un destinataire relevant de la juridiction d'une autre Partie à la Convention ne peut pas être interdit ou soumis à une autorisation spéciale aux seules fins de la protection des données. Toutefois ce principe de la libre circulation des données entre les Parties présumant un niveau de protection des données équivalent n'est pas absolu. Il souffre un bémol puisqu'il réserve la situation où une Partie à la Convention est régie par des règles de protection harmonisées contraignantes et communes à des Etats appartenant à une organisation internationale régionale. En clair, il s'agit, par cette disposition, de préserver le mécanisme d'adéquation de l'Union européenne et d'éviter que des données soient transférées sans autre garantie vers une Partie non membre de l'Union européenne qui ne serait pas au bénéfice d'une décision d'adéquation. Cette différenciation suscite des critiques de la part de certains Etats hors de l'Union européenne, voire hors de l'Europe. Elle pourrait être un obstacle à l'attractivité de la Convention à l'égard d'Etat non membre du Conseil de l'Europe, mais susceptible d'adhérer à la Convention. Pour atténuer ce risque, il faut dès lors souhaiter que l'adhésion à la Convention soit un facteur prépondérant dans la recon-



naissance de l'adéquation. Une déclaration d'intention en ce sens de l'Union européenne serait un signe positif à l'égard des Etats tiers. Un premier pas a été fait avec une communication de la commission du 29 novembre 2013 au Parlement européen et au Conseil concernant les flux de données entre l'Union européenne et les Etats-Unis dans laquelle la commission estime qu'il faut favoriser l'adhésion d'Etat tiers à la Convention⁶. En outre, il est important que les exigences d'appréciation du niveau de protection des données 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 29⁷ 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 conventionnel.

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 approprié est garanti. Ce niveau doit être d'une certaine qualité afin de garantir que les droits de l'homme ne soient pas affectés par la mondialisation et la nature transfrontalière des flux de données. Ce niveau de protection approprié 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 ad hoc 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. Pour les flux de données vers des Etats parties à la Convention qui ne sont pas membres de l'Union européenne et

⁶ Communication from the Commission to the European Parliament and the Council Rebuilding Trust in EU-US Data Flows, st17067/13

⁷ 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. »



qui ne sont pas encore au bénéfice d'une décision d'adéquation, les transferts devront être encadrés par des mesures standardisées ou ad'hoc.

En l'absence d'un niveau de protection des données approprié, 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 en présence d'intérêts légitimes prépondérants, notamment des intérêts publics importants prévus par la loi et qui constituent une mesure nécessaire dans une société démocratique. On pense notamment aux nécessités de la coopération policière ou judiciaire en matière pénale. Ces transferts en l'absence d'un niveau de protection approprié ne doivent pas intervenir de manière régulière, mais couvrir des situations particulières.

Le projet introduit, à l'article 9, 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.

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 dispositions 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 dans l'accomplissement de leurs fonctions et l'exercice de leurs pouvoirs, 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. L'institutionnalisation de la coopération entre autorités de contrôle est indispensable pour faire face à l'internationalisation des traitements de données personnelles afin d'assurer une plus grande effectivité au droit à la protection des données. Le projet prévoit que pour faciliter cette coordination, les autorités de contrôle peuvent se constituer en conférence ou en réseau. 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 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 préalablement 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 une 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 de protection des données. 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 approprié. Pour apprécier ce niveau, 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 Conseil de l'Europe. Après avoir été adopté par le comité consultatif lors de la 29^e réunion plénière en novembre 2012, le projet est maintenant examiné par le CAHDATA. Ce comité est composé de l'ensemble des pays membres du Conseil de l'Europe, de l'Uruguay, partie à la Convention, des pays observateurs permanents au Conseil de l'Europe et d'un certain nombre d'Etats invités et susceptibles l'adhérer à la Convention. La Commission européenne ainsi que des représentants de la société civile et



économique participent aux travaux. Le comité doit préparer un protocole d'amendement à la convention sur la base du projet du T-PD. Le projet devrait être finalisé dans le courant 2014 et transmis au comité des Ministres pour adoption et ouverture à la procédure d'acceptation par les Parties.

Avec cette modernisation, la convention 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 appelée 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 offre aux Etats tiers en y adhérant une opportunité de se voir reconnaître adéquat par l'Union européenne. Dans le contexte actuel d'un affaiblissement manifeste de nos droits et de nos libertés fondamentales au profit de la sécurité et face aux dérives vers une surveillance de masse généralisée, il est urgent de renforcer le cadre juridique de la protection des données en Europe et dans le monde. L'adoption de la Convention modernisée et ouverte au monde constituera un pas important dans ce sens.